Service de sécurité géré du gouvernement du Canada (SSGGC)

Appendice D : Catalogue des contrôles de sécurité ITSG-33 – Annexe 3, version provisoire 3.1

Date : 15 juin 2012

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

Conseils en matière de sécurité des TI

Guide de gestion des risques de sécurité des systèmes d'information

Catalogue des contrôles de sécurité

ITSG-33 – Annexe 3

ÉBAUCHE 3.1

24 Septembre 2010

Canada

Page intentionnellement laissée en blanc.

Avant-propos

Le document *Annexe 3 du Guide de gestion des risques de sécurité des systèmes d'information (ITSG-33)* est non classifié et il est publié sous l'autorité du chef du Centre de la sécurité des télécommunications Canada (CSTC).

Les propositions de modification doivent être envoyées au représentant des Services à la clientèle du CSTC affecté au ministère.

Les demandes d'exemplaires additionnels ou de modification à apporter à la distribution doivent être soumises à votre représentant des Services à la clientèle du CSTC.

Pour de plus amples renseignements, prière de communiquer avec les Services à la clientèle de la Sécurité des TI du CSTC, par courriel à l'adresse client.svcs@cse-cst.gc.ca.

Date d'entrée en vigueur

Cette publication entre en vigueur en MOIS 2010.

Colleen D'Iorio

Directrice générale, Cyberprotection, Sécurité des TI

Résumé

Cette publication s'inscrit dans le cadre d'évaluation et d'autorisation de la sécurité publié par le Centre de la sécurité des télécommunications Canada (CSTC) dans le document *Guide de gestion des risques de sécurité des systèmes d'information* (ITSG-33), Conseils en matière de sécurité des TI. Il contient des définitions des contrôles de sécurité que les praticiens du domaine peuvent utiliser comme base de sélection des contrôles servant à protéger les systèmes d'information du gouvernement du Canada (GC).

Elle inclut des définitions des contrôles de sécurité qui peuvent être retenus pour assurer la protection des systèmes d'information du GC, de niveau de sensibilité et de criticité de très faible à très élevé, exploités dans des domaines classifiés, protégés et non classifiés. La publication peut aider les praticiens de la sécurité durant le processus de mise en œuvre de la sécurité de l'information lors de la sélection des contrôles de sécurité de systèmes d'information particuliers. Le catalogue peut également servir de base au développement de profils de protection pour des types de système d'information spécifiques ou des collectivités particulières d'utilisateurs.

Le catalogue définit trois classes générales de contrôles de sécurité : technique, opérationnelle et gestion. Conformément à la portée de ce document, les contrôles de sécurité sont utilisés exclusivement pour protéger l'information et les systèmes d'information.

Ce document a été préparé en tenant compte du cadre législatif et stratégique existant du GC au moment de sa publication, plus particulièrement la *Politique sur la sécurité du gouvernement* [Référence 1]. En cas de divergence ou de conflit d'interprétation entre les contrôles de sécurité définis dans le présent document et les lois et les politiques du GC ainsi que les politiques, directives et normes du Secrétariat du Conseil du Trésor du Canada (SCT), ces dernières ont préséance.

L'Annexe 2 de la publication, qui décrit une recommandation de processus de mise en œuvre de la sécurité de l'information, inclut des conseils sur la façon d'utiliser le catalogue pour sélectionner les contrôles de sécurité et les améliorations de contrôle pour les systèmes d'information. Voir à la section 1.4 la liste des publications connexes.

Ce catalogue est essentiellement le même que celui publié aux É.-U. par le National Institute of Standards and Technology (NIST) dans le document Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* [Référence 2], incluant les mises à jour du 05-01-2010. Les définitions des contrôles ont été légèrement modifiées pour tenir contexte du GC, et de nouveaux contrôles, clairement identifiés, ont été ajoutés afin d'harmoniser le catalogue avec les lignes directrices du cadre de développement du CSTC concernant l'architecture de sécurité d'entreprise (ASE).

Historique des révisions

Document n°	Changements	
EBAUCHE 3.1	Ajout de nouvelles améliorations des contrôles de sécurité : IA-2 (100), AC-17 (100). Clarification de l'amélioration du contrôle de sécurité : PE-6 (2).	

Table des matières

Liste des tableaux

Liste des figures

Liste des abréviations et acronymes

ASCII	Code ASCII (American Standard Code for Information Interchange)
BCP	Bureau du Conseil privé
CAAR	Contrôles d'accès axés sur les rôles
CDS	Cycle de développement des systèmes
CEE	Norme CEE (Common Event Expression)
CIP	Connexion Internet protégée
CNB	Code national du bâtiment
CNPI	Code national de prévention des incendies
CNSS	Committee on National Security Systems
COMSEC	Sécurité des communications
CONOPS	Concept d'opération
COTS	Produit commercial
CSTC	Centre de la sécurité des télécommunications Canada
CUI	Controlled Unclassified Information
CVC	Chauffage, ventilation et climatisation
CVE	Common Weakness Enumeration
CWE	Common Vulnerabilities and Exposures
DAC	Contrôle d'accès discrétionnaire
DHCP	Protocole DHCP (Dynamic Host Control Protocol)

DMZ	Zone démilitarisée
DNS	Système DNS (Domaine Name System)
É.-U.	États-Unis
EAP	Protocole EAP (Extensible Authentification Protocol)
FIPS	Federal Information Processing Standards
FTP	Protocole FTP (File Transfer Protocol)
GC	Gouvernement du Canada
GOTS	Produit du gouvernement
GSTI	Gestion de la sécurité des technologies de l'information
HTTP	Protocole HTTP (Hypertext Transfer Protocol)
ICP	Infrastructure à clé publique
ID	Identificateur
IEEE	Institute of Electrical and Electronics Engineers
IP	Protocole IP
IPv6	Protocole IP Version 6
ITSB	Bulletins de sécurité des TI
ITSD	Directives en matière de sécurité des TI
ITSG	Conseils en matière de sécurité des TI
MAC	Contrôle d'accès obligatoire
MAC	Protocole MAC (Media Access Control)
MLS	Multilevel Secure
MSL	Multiple Security level
NIP	Numéro d'identification personnelle
NIST	National Institute of Standards and Technology
PCA	Planification de la continuité des activités
PDF	Format PDF (Portable Document Format)
PEAP	Protocole PEAP (Protected Extensible Authentification Protocol)
PSG	Politique sur la sécurité du gouvernement
PUB	Publication
RCMP	Gendarmerie royale du Canada
RPV	Réseau privé virtuel

SCAP	Protocole SCAP (Security contenu Automation Protocol)
SCI	Renseignements cloisonnés de nature délicate
SCT	Secrétariat du Conseil du Trésor
SIM	Security Information Management
SSH	Protocole SSH (Secure Shell)
STIG	Security Technical Implementation Guide
TCP	Protocole TCP (Transmission Control Protocol)
TLS	Protocole TLS (Transport Layer Security)
TMG	Temps moyen de Greenwich
TPSGC	Travaux publics et Services gouvernementaux Canada
TUC	Temps universel coordonné
UHF	Ultra-haute fréquence
URL	Adresse URL (Uniform Ressource Locator)
USB	Bus USB (Universal Serial Bus)
UUENCODE	UNIX to UNIX Encoding
VHF	Très haute fréquence
VoIP	Voix sur IP
XML	Langage XML (eXtensible Markup Language)

1. Introduction

1.1 But

Cette publication s'inscrit dans le cadre d'évaluation et d'autorisation de la sécurité publié par le Centre de la sécurité des télécommunications Canada (CSTC) dans le document *Guide de gestion des risques de sécurité des systèmes d'information* (ITSG-33), Conseils en matière de sécurité des TI. Il contient des définitions des contrôles de sécurité que les praticiens du domaine peuvent utiliser comme base de sélection des contrôles servant à protéger les systèmes d'information du gouvernement du Canada (GC).

Le catalogue des contrôles de sécurité :

- Appuie indirectement les lois du GC et les politiques, directives et normes du Secrétariat du Conseil du Trésor du Canada (SCT) en matière de protection de l'information et des systèmes d'information.
- Offre pour les systèmes d'information des contrôles de sécurité qui répondent aux besoins de protection actuels des ministères ainsi qu'aux exigences et technologies en constante évolution du futur.
- Facilite une approche comparative plus uniforme et reproductible pour la sélection et la spécification des contrôles de sécurité pour les systèmes d'information du GC.
- Crée une base de développement de méthodes et de procédures d'évaluation de l'efficacité des contrôles de sécurité.
- Améliore la communication en proposant un lexique commun qui facilite la discussion des concepts de gestion des risques.

1.2 Portée et applicabilité

La publication inclut des définitions des contrôles de sécurité qui peuvent être retenus pour assurer la protection des systèmes d'information du GC, de niveau de sensibilité et de criticité de très faible à très élevé, exploités dans des domaines classifiés, protégés et non classifiés.

Elle peut aider les praticiens de la sécurité durant le processus de mise en œuvre de la sécurité de l'information lors de la sélection des contrôles de sécurité de systèmes d'information particuliers. Le catalogue peut également servir de base au développement de profils de protection pour des types de système d'information spécifiques ou des collectivités particulières d'utilisateurs.

Conformément à la portée de ce document, les contrôles de sécurité sont utilisés exclusivement pour protéger l'information et les systèmes d'information.

Ce document a été préparé en tenant compte du cadre législatif et stratégique existant du GC au moment de sa publication, plus particulièrement la *Politique sur la sécurité du gouvernement* [Référence 1]. En cas de divergence ou de conflit d'interprétation entre les contrôles de sécurité définis dans le présent document et les lois et les politiques du GC ainsi que les politiques, directives et normes du SCT, ces dernières ont préséance.

1.3 Public cible

Ce document vise un public varié de praticiens de la sécurité, incluant :

- Les responsables de la gestion et de la surveillance de la sécurité de l'information et des systèmes d'information (p. ex., agents de la sécurité ministérielle, dirigeants principaux de l'information, directeurs des techniques informatiques, gestionnaires de système d'information, gestionnaires de la sécurité de l'information).
- Les responsables du développement et de la mise en œuvre des systèmes d'information (p. ex., gestionnaires de projet, techniciens des systèmes d'information, techniciens en sécurité des systèmes d'information, concepteurs et développeurs de systèmes d'information).
- Les responsables opérationnels de la sécurité de l'information (p. ex., propriétaires, administrateurs et agents de sécurité de système d'information).
- Les responsables de la surveillance et de l'évaluation de la sécurité de l'information et des systèmes d'information (p. ex., vérificateurs, évaluateurs de la sécurité).

1.4 Publications connexes

Cette publication fait partie des lignes directrices du CSTC en matière d'autorisation et d'évaluation de la sécurité. Les autres lignes directrices sont énoncées dans les publications suivantes :

- ITSG-33 – Guide de gestion des risques de sécurité des systèmes d'information
- ITSG-33, Annexe 1 – Glossaire
- ITSG-33, Annexe 2 – Processus de mise en œuvre de la sécurité de l'information
- ITSG-33, Annexe 4 – Profils de contrôle de sécurité des systèmes d'information protégés B

1.5 Structure de la publication

La suite de la publication est organisée comme suit :

- Section 2 – Organisation des contrôles de sécurité.
- Section 3 – Définitions des contrôles de sécurité.
- Section 4 – Références.
- Appendice A – Associe les contrôles de sécurité aux objectifs de confidentialité, d'intégrité et de disponibilité correspondants.

2. Organisation de la publication

2.1 Catalogue des contrôles de sécurité

Cette publication est un catalogue des contrôles de sécurité techniques, opérationnels et de gestion pour les systèmes d'information. Son but est de servir de base à la sélection des contrôles de sécurité pour protéger les systèmes d'information du GC. Ce catalogue est essentiellement le même que celui publié aux É.-U. par le National Institute of Standards and Technology (NIST) dans le document Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* [Référence 2], incluant les mises à jour du 05-01-2010. Les définitions des contrôles ont été légèrement modifiées et développées pour tenir compte du contexte du GC.

Les contrôles définis dans le catalogue sont divisés en classes et familles, tel qu'illustré dans la Figure 1. Chacun de ces éléments est décrit en détail dans les sous-sections ci-dessous.

Classes	Technique	Opérationnelle	Gestion
Familles	AC - Contrôle d'accès	AT - Sensibilisation et formation	CA - Évaluation et autorisation de sécurité
	AU - Vérification et responsabilité	CM - Gestion de la configuration	PL - Planification
	IA - Identification et authentification	CP - Planification d'urgence	RA - Évaluation du risque
	SC - Protection des systèmes et des communications	IR - Intervention en cas d'incident	SA - Acquisition des systèmes et des services
		MA - Maintenance	PM - Gestion des programmes
		MP - Protection des supports	
		PE - Protection physique et environnementale	
		PS - Sécurité du personnel	
		SI - Intégrité des systèmes et de l'information	

Figure 1 – Structure du catalogue des contrôles de sécurité

2.2 Classes

Le catalogue définit trois classes générales de contrôles de sécurité : technique, opérationnelle et gestion. Les définitions de ces classes sont extraites de la publication 200 du FIPS (Federal Information Processing Standards), *Minimum Security Controls Requirements for Federal Information and Information Systems* [Référence 5] :

- **Contrôles de sécurité de gestion** : contrôles (c.-à-d., mesures de protection ou contremesures) axés sur la gestion du risque et la gestion de la sécurité des systèmes d'information.
- **Contrôles de sécurité opérationnels** : contrôles dont la mise en œuvre et l'exécution relèvent des individus (plutôt que des systèmes).
- **Contrôles de sécurité techniques** : contrôles principalement mis en œuvre et exécutés par les mécanismes des composantes matérielles, logicielles et micrologicielles des systèmes d'information.

Il importe de mentionner que les définitions des classes de contrôles ne sont pas exclusives. Dans certains cas, pour appliquer les fonctions de sécurité qui leur ont été assignées, les contrôles techniques peuvent exiger du personnel qu'il exécute des procédures manuelles alors que les contrôles opérationnels peuvent recourir à la technologie intégrée aux systèmes d'information.

2.3 Familles

Chaque classe de contrôles de sécurité est ensuite divisée en familles. La classe technique inclut les familles de contrôles suivantes :

- **Contrôle d'accès :** contrôles qui permettent d'autoriser ou d'interdire l'accès des ressources du système d'information à l'utilisateur.
- **Vérification et responsabilisation** : contrôles qui permettent de collecter, d'analyser et de stocker les dossiers de vérification associés aux opérations que l'utilisateur exécute dans le système d'information.
- **Identification et authentification** : contrôles qui permettent de vérifier l'identification unique et l'authentification des utilisateurs qui tentent d'accéder au système d'information.
- **Protection des systèmes et des communications** : contrôles qui permettent de protéger le système d'information lui-même ainsi que ses communications internes et externes.

La classe des contrôles de sécurité opérationnels inclut les familles de contrôles suivantes :

- **Sensibilisation et formation** : contrôles qui concernent l'éducation des utilisateurs à la sensibilisation à la sécurité des systèmes d'information.
- **Gestion de la configuration** : contrôles qui permettent la gestion et le contrôle de toutes les composantes du système d'information (p. ex., matériel, logiciel et éléments de configuration).
- **Planification d'urgence** : contrôles qui permettent d'assurer la disponibilité des services du système d'information dans l'éventualité d'une panne de composante ou d'un désastre.
- **Intervention en cas d'incident** : contrôles qui permettent de détecter les incidents de sécurité liés au système d'information, d'intervenir, le cas échéant, et de produire les rapports pertinents.
- **Maintenance** : contrôles qui permettent d'assurer la maintenance du système d'information et sa disponibilité permanente.
- **Protection des supports** : contrôles qui permettent de protéger les supports du système d'information (p. ex., disques et bandes) durant tout leur cycle de vie.
- **Protection physique et environnementale** : contrôles liés à l'accès physique d'un système d'information et à la protection de l'équipement environnemental auxiliaire (c.-à-d., alimentation, climatisation, câblage) servant à son exploitation.
- **Sécurité du personnel** : contrôles qui appliquent les procédures qui permettent de s'assurer que tout le personnel qui a accès au système d'information possède les autorisations requises ainsi que les cotes de sécurité appropriées.

- **Intégrité de l'information et des systèmes** : contrôles qui permettent de protéger l'intégrité des composantes du système d'information et de l'information traitée.

La classe des contrôles de sécurité de gestion inclut les familles de contrôles suivantes :

- **Évaluation et autorisation de sécurité** : contrôles qui concernent l'évaluation et l'autorisation de sécurité du système d'information.
- **Planification** : contrôles qui concernent les activités de planification de la sécurité, incluant les évaluations des facteurs relatifs à la vie privée.
- **Évaluation des risques** : contrôles qui concernent l'exécution des évaluations de risques et de l'analyse des vulnérabilités.
- **Acquisition des systèmes et des services** : contrôles qui concernent la passation de marchés pour l'acquisition des produits et des services nécessaires au soutien de la mise en œuvre et de l'exploitation du système d'information.
- **Gestion des programmes** : contrôles de gestion des programmes de sécurité de l'information qui ciblent les exigences organisationnelles de sécurité indépendantes des systèmes d'information et essentielles à la gestion des programmes.

Le Tableau 2 inclut la liste des contrôles de sécurité existants de chaque classe et famille de contrôles.

À l'occasion, au fur et à mesure de l'évolution de la technologie, des menaces et des contremesures, le NIST annule certains contrôles de sécurité mais les conserve dans son catalogue afin de préserver la stabilité des identificateurs de contrôle utilisés dans les plans de sécurité et d'assurer le soutien des outils de mise en œuvre tels les matrices de traçabilité et les outils automatisés de gestion des risques. Les contrôles de sécurité annulés sont également conservés aux mêmes fins dans le présent catalogue.

2.4 Contrôles de sécurité

L'exemple de contrôle de sécurité (PE-2 Autorisations d'accès physique) à la page suivante illustre les différentes composantes servant à définir ce type de contrôle :

- Numéro du contrôle : on attribue à chaque contrôle un numéro unique (p. ex., PE-2). **Tous les contrôles dont le numéro commence à la valeur 100 (**p. ex.**, SC-100) sont des contrôles de sécurité propres au Canada**. Les contrôles de la série 100 ont été ajoutés en sus des contrôles de sécurité du NIST 800-53 afin de tenir compte des exigences spécifiques du GC. Lorsque le nom d'un contrôle canadien diffère du nom original attribué par le NIST, ce dernier (traduit) est indiqué entre crochets après le nom canadien. Exemple : Plan de mise en œuvre des mesures de protection (Plan d'action et jalons).
- Section *Contrôle* : inclut une description du contrôle formulée à l'aide d'un ou de plusieurs énoncés concis de la capacité de sécurité spécifique requise pour protéger un aspect d'un système d'information. On attribue une désignation alphabétique distincte (p. ex., (A), (B), etc.) à chaque énoncé; l'énoncé doit être respecté pour que le contrôle de sécurité correspondant soit appliqué. **Tous les énoncés qui commencent par AA (**p. ex.**, SC-10 (AA)) sont propres au Canada**. Les énoncés de contrôle de sécurité de la série AA ont été ajoutés en sus des énoncés du NIST 800-53 afin de tenir compte des exigences spécifiques du GC.
- Section *Conseils supplémentaires* optionnelle : inclut de l'information supplémentaire sur le contrôle pour en faciliter la mise en œuvre, incluant de l'information sur tout autre contrôle de sécurité connexe. Cette section n'inclut aucun énoncé auquel on doit se conformer pour mettre le contrôle en œuvre.
- Section *Améliorations du contrôle* optionnelle : inclut une définition, formulée à l'aide d'énoncés concis, des capacités de sécurité supplémentaires qui permettent d'accroître la force d'un contrôle de sécurité. On attribue à chaque amélioration une désignation numérique distincte (p. ex., (1), (2), etc.). **Toutes les améliorations dont le numéro commence à la valeur 100 (**p. ex.**, PE-2 (100)) sont des améliorations propres au Canada**. Les améliorations de la série 100 ont été ajoutées en sus des améliorations du NIST 800-53 afin de tenir compte des exigences spécifiques du GC.
- Section *Conseils supplémentaires d'amélioration* : inclut de l'information détaillée supplémentaire sur les améliorations, incluant de l'information sur tout autre contrôle de sécurité correspondant. Cette section n'inclut aucune amélioration supplémentaire à laquelle on doit se conformer pour mettre l'amélioration du contrôle en œuvre.
- Section *Références* : inclut des références aux politiques, directives, normes et lignes directrices qui concernent le contrôle de sécurité. Cette section vise à fournir de l'information supplémentaire ou un contexte que le lecteur peut juger utiles pour sélectionner et mettre en œuvre le contrôle concerné. La portée de la référence peut être de nature générale ou spécifique, selon le type de contrôle (p. ex., lignes directrices du GC sur l'authentification ou norme technique de configuration de la sécurité).

Plusieurs des contrôles et des améliorations contiennent des paramètres de contrôle définis par l'organisation. Ce sont essentiellement des paramètres substituables que les praticiens de la sécurité

peuvent préciser durant la sélection des valeurs de processus propres au contexte de leur organisation. L'amélioration de contrôle qui suit, tirée du contrôle PE-2, est un bon exemple de paramètres définis par l'organisation :

> L'organisation examine et approuve la liste d'accès et les justifi catifs d'autorisation [*Affectation : fréquence définie par l'organisation*], et supprime de la liste les emplo yés qui n'ont plus besoin de droit d'accès.

Dans ce cas-ci, les praticiens de la sécurité doivent préciser la fréquence réelle dans le processus de sélection du contrôle de sécurité. S'il n'existe pas déjà de profil de sécurité contenant les valeurs de paramètre appropriées, les politiques, normes et lignes directrices du GC ainsi que leur propre expérience peuvent aider les praticiens à définir ces spécifications.

PE-2 AUTORISATIONS D'ACCÈS PHYSIQUE

Contrôle :

(A) L'organisation développe et tient à jour une liste des employés autorisés à accéder à l'installation qui héberge le système d'information (sauf dans les cas où l'installation est officiellement accessible au public).

(B) L'organisation émet des justificatifs d'autorisation.

(C) L'organisation examine et approuve la liste d'accès et les justificatifs d'autorisation [*Affectation : fréquence définie par l'organisation*], et supprime de la liste les employés qui n'ont plus besoin de droit d'accès.

Conseils supplémentaires : Les justificatifs d'autorisation incluent, par exemple, les badges, les cartes d'identité et les cartes à puce. Contrôles connexes : PE-3, PE-4.

Améliorations du contrôle :

(1) L'organisation autorise, selon le poste ou le rôle de l'employé, l'accès physique à l'installation qui héberge le système d'information.

(2) L'organisation exige deux formes d'identification pour permettre l'accès à l'installation.

Conseils supplémentaires d'amélioration : Exemples de formes d'identification : badge d'identification, carte-clé, NIP encodé et données biométriques.

(100) L'organisation restreint l'accès à une installation qui héberge un système de traitement d'information classifiée aux seuls employés autorisés qui possèdent une cote de sécurité appropriée et une autorisation d'accès.

Références :

Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7].

2.5 Utilisation du catalogue

L'Annexe 2 de la publication, qui décrit une recommandation de processus de mise en œuvre de la sécurité de l'information, inclut des conseils sur la façon d'utiliser le catalogue pour sélectionner les contrôles de sécurité et les améliorations de contrôle pour les systèmes d'information. Voir à la section 1.4 la liste des publications connexes.

2.6 Codes de priorité

Un *code de priorité* est attribué à chaque contrôle de sécurité. Les organisations peuvent utiliser le code recommandé de chaque contrôle pour les aider à prendre des décisions concernant l'ordre de mise en œuvre des contrôles (p. ex., la mise en œuvre d'un contrôle dont le code de priorité est 1 (P1) a une priorité supérieure à celle d'un contrôle dont le code de priorité est 2 (P2), et la mise en œuvre d'un contrôle dont le code de priorité est 2 (P2) a une priorité supérieure à celle d'un contrôle dont le code de priorité est 3 (P3)). Un code de priorité non précisé (P0) n'a aucune incidence sur les décisions. Si l'utilisateur choisit un contrôle qui n'est pas un contrôle de sécurité de base, le code de priorité (P0) est attribué par défaut. Un examen est ensuite effectué pour attribuer au contrôle un code de priorité approprié en fonction des autres contrôles de sécurité. Le code retenu peut être (P1), (P2) ou (P3). Voir le Tableau 1.

Cette priorisation recommandée de l'ordre de mise en œuvre des contrôles permet de s'assurer que les contrôles de base, dont dépendent d'autres contrôles, sont appliqués en premier afin de permettre aux organisations de déployer les contrôles de manière structurée et en temps opportun, en fonction des ressources disponibles. La mise en œuvre ordonnée des contrôles ne signifie pas qu'il faut atteindre un niveau d'atténuation de risque particulier avant de mettre en œuvre tous les contrôles prévus dans le plan de sécurité. **Les codes de priorité servent uniquement à établir l'ordre de mise en œuvre et non à prendre des décisions concernant la sélection des contrôles**. Les attributions de codes de priorité aux contrôles de sécurité sont précisées dans le Tableau 2.

Tableau 1 – Codes de priorité des contrôles de sécurité

Code de priorité	Ordre	Mesure
Code de priorité 1 (P1)	EN PREMIER	Mise en œuvre des contrôles de sécurité P1 en premier.
Code de priorité 2 (P2)	APRÈS	Mise en œuvre des contrôles de sécurité P2 après celle des contrôles P1.
Code de priorité 3 (P3)	EN DERNIER	Mise en œuvre des contrôles de sécurité P3 après celle des contrôles P1 et P2.
Code de priorité non précisé (P0)	AUCUN	Aucun code de priorité précisé pour ce contrôle de sécurité.

Tableau 2 – Classes, familles et codes de priorité des contrôles de sécurité

Contrôle n°	Code de priorité	Nom du contrôle	Classe
AC - Contrôle d'accès			
AC-1	P1	Politique et procédures de contrôle d'accès	Technique
AC-2	P1	Gestion des comptes	Technique
AC-3	P1	Application des droits d'accès	Technique
AC-4	P1	Application des contrôles de flux d'information	Technique
AC-5	P1	Séparation des tâches	Technique

Contrôle n°	Code de priorité	Nom du contrôle	Classe
AC-6	P1	Privilège minimum	Technique
AC-7	P2	Tentatives de connexion non réussies	Technique
AC-8	P1	Avis concernant l'utilisation du système	Technique
AC-9	P0	Avis concernant les connexions antérieures (accès)	Technique
AC-10	P2	Contrôle des sessions simultanées	Technique
AC-11	P3	Verrouillage de session	Technique
AC-12	-	[ANNULÉ]	-
AC-13	-	[ANNULÉ]	-
AC-14	P1	Opérations permises sans identification ni authentification	Technique
AC-15	-	[ANNULÉ]	-
AC-16	P1	Attributs de sécurité	Technique
AC-17	P1	Accès à distance	Technique
AC-18	P1	Accès sans fil	Technique
AC-19	P1	Contrôle d'accès aux dispositifs mobiles	Technique
AC-20	P1	Utilisation des systèmes d'information externes	Technique
AC-21	P0	Collaboration et partage d'information entre utilisateurs	Technique
AC-22	P2	Contenu accessible au public	Technique
AT - Sensibilisation et formation			
AT-1	P1	Politique et procédures de formation et de sensibilisation à la sécurité	Opérationnelle
AT-2	P1	Sensibilisation à la sécurité	Opérationnelle
AT-3	P1	Formation à la sécurité	Opérationnelle
AT-4	P3	Dossiers de formation à la sécurité	Opérationnelle
AT-5	P0	Contacts avec les groupes et associations de sécurité	Opérationnelle
AU - Vérification et responsabilisation			
AU-1	P1	Politique et procédures de vérification et de responsabilisation	Technique
AU-2	P1	Événements vérifiables	Technique
AU-3	P1	Contenu des dossiers de vérification	Technique
AU-4	P1	Capacité de stockage des vérifications	Technique
AU-5	P1	Intervention en cas de problèmes de traitement	Technique
AU-6	P1	Examen, analyse et rapports de vérification	Technique
AU-7	P2	Réduction des vérifications et production des rapports	Technique
AU-8	P1	Timbres horodateurs	Technique
AU-9	P1	Protection de l'information de vérification	Technique
AU-10	P1	Non-répudiation	Technique
AU-11	P3	Conservation des dossiers de vérification	Technique
AU-12	P0	Production des dossiers de vérification	Technique
AU-13	P0	Surveillance de la divulgation d'information	Technique
AU-14	P0	Vérification des sessions	Technique
CA – Évaluation et autorisation de sécurité			
CA-1	P1	Politique et procédures d'évaluation et d'autorisation de la sécurité	Gestion
CA-2	P2	Évaluations de la sécurité	Gestion

Contrôle n°	Code de priorité	Nom du contrôle	Classe
CA-3	P1	Connexions des systèmes d'information	Gestion
CA-4	-	[ANNULÉ]	-
CA-5	P3	Plan d'action et jalons	Gestion
CA-6	P3	Autorisation de sécurité	Gestion
CA-7	P3	Surveillance permanente	Gestion
CM - Gestion de la configuration			
CM-1	P1	Politique et procédures de gestion de la configuration	Opérationnelle
CM-2	P1	Configuration de base	Opérationnelle
CM-3	P1	Contrôle des modifications de la configuration	Opérationnelle
CM-4	P2	Analyse des répercussions sur la sécurité	Opérationnelle
CM-5	P1	Restrictions d'accès associées aux modifications	Opérationnelle
CM-6	P1	Paramètres de configuration	Opérationnelle
CM-7	P1	Fonctionnalité minimale	Opérationnelle
CM-8	P1	Inventaire des composantes de système d'information	Opérationnelle
CM-9	P1	Plan de gestion de la configuration	Opérationnelle
CP - Planification d'urgence			
CP-1	P1	Politique et procédures de planification d'urgence	Opérationnelle
CP-2	P1	Plan des mesures d'urgence	Opérationnelle
CP-3	P2	Formation sur les situations d'urgence	Opérationnelle
CP-4	P2	Tests et exercices relatifs au plan des mesures d'urgence	Opérationnelle
CP-5	-	[ANNULÉ]	-
CP-6	P1	Sites de stockage de secours	Opérationnelle
CP-7	P1	Site de traitement de secours	Opérationnelle
CP-8	P1	Services de télécommunications	Opérationnelle
CP-9	P1	Sauvegarde des systèmes d'information	Opérationnelle
CP-10	P1	Récupération et reconstitution des systèmes d'information	Opérationnelle
IA - Identification et authentification			
IA-1	P1	Politique et procédures d'identification et d'authentification	Technique
IA-2	P1	Identification et authentification (utilisateurs organisationnels)	Technique
IA-3	P1	Identification et authentification des dispositifs	Technique
IA-4	P1	Gestion des identificateurs	Technique
IA-5	P1	Gestion des authentifiants	Technique
IA-6	P1	Occultation des authentifiants	Technique
IA-7	P1	Authentification des modules cryptographiques	Technique
IA-8	P1	Identification et authentification (utilisateurs non organisationnels)	Technique
IR - Intervention en cas d'incident			
IR-1	P1	Politique et procédures d'intervention en cas d'incident	Opérationnelle
IR-2	P2	Formation sur les interventions en cas d'incident	Opérationnelle
IR-3	P2	Tests et exercices relatifs aux interventions en cas d'incident	Opérationnelle
IR-4	P1	Traitement des incidents	Opérationnelle
IR-5	P1	Surveillance des incidents	Opérationnelle
IR-6	P1	Signalement des incidents	Opérationnelle

Contrôle n°	Code de priorité	Nom du contrôle	Classe
IR-7	P3	Assistance pour les interventions en cas d'incident	Opérationnelle
IR-8	P1	Plan d'intervention en cas d'incident	Opérationnelle
MA - Maintenance			
MA-1	P1	Politique et procédures de maintenance des systèmes	Opérationnelle
MA-2	P2	Maintenance contrôlée	Opérationnelle
MA-3	P2	Outils de maintenance	Opérationnelle
MA-4	P1	Maintenance effectuée à distance	Opérationnelle
MA-5	P1	Personnel de maintenance	Opérationnelle
MA-6	P1	Maintenance opportune	Opérationnelle
MP - Protection des supports			
MP-1	P1	Politique et procédures de protection des supports	Opérationnelle
MP-2	P1	Accès aux supports	Opérationnelle
MP-3	P1	Marquage des supports	Opérationnelle
MP-4	P1	Entreposage des supports	Opérationnelle
MP-5	P1	Transport des supports	Opérationnelle
MP-6	P1	Nettoyage des supports	Opérationnelle
PE - Protection physique et environnementale			
PE-1	P1	Politique et procédures de protection physique et environnementale	Opérationnelle
PE-2	P1	Autorisations d'accès physique	Opérationnelle
PE-3	P1	Contrôle d'accès physique	Opérationnelle
PE-4	P1	Contrôle d'accès aux supports de transmission	Opérationnelle
PE-5	P1	Contrôle d'accès aux dispositifs de sortie	Opérationnelle
PE-6	P1	Surveillance de l'accès physique	Opérationnelle
PE-7	P1	Contrôle des visiteurs	Opérationnelle
PE-8	P3	Dossiers d'accès	Opérationnelle
PE-9	P1	Équipement et câblage d'alimentation	Opérationnelle
PE-10	P1	Arrêt d'urgence	Opérationnelle
PE-11	P1	Alimentation d'urgence	Opérationnelle
PE-12	P1	Éclairage d'urgence	Opérationnelle
PE-13	P1	Protection contre les incendies	Opérationnelle
PE-14	P1	Contrôle de la température et de l'humidité	Opérationnelle
PE-15	P1	Protection contre les dégâts d'eau	Opérationnelle
PE-16	P1	Livraison et retrait	Opérationnelle
PE-17	P1	Lieu de travail de secours	Opérationnelle
PE-18	P2	Emplacement des composantes de système d'information	Opérationnelle
PE-19	P0	Fuites d'information	Opérationnelle
PL - Planification			
PL-1	P1	Politique et procédures de planification de la sécurité	Gestion
PL-2	P1	Plan de sécurité des systèmes	Gestion
PL-3	-	[ANNULÉ]	-
PL-4	P1	Règles de conduite	Gestion
PL-5	P1	Évaluation des facteurs relatifs à la vie privée	Gestion

Contrôle n°	Code de priorité	Nom du contrôle	Classe
PL-6	P3	Planification des activités relatives à la sécurité	Gestion
PS - Sécurité du personnel			
PS-1	P1	Politique et procédures de sécurité du personnel	Opérationnelle
PS-2	P1	Catégorisation des postes	Opérationnelle
PS-3	P1	Enquête de sécurité sur le personnel	Opérationnelle
PS-4	P2	Licenciement du personnel	Opérationnelle
PS-5	P2	Transfert de personnel	Opérationnelle
PS-6	P3	Ententes d'accès	Opérationnelle
PS-7	P1	Sécurité du personnel tiers	Opérationnelle
PS-8	P3	Sanctions imposées au personnel	Opérationnelle
RA - Évaluation des risques			
RA-1	P1	Politique et procédures d'évaluation des risques	Gestion
RA-2	P1	Catégories de sécurité	Gestion
RA-3	P1	Évaluation des risques	Gestion
RA-4	-	[ANNULÉ]	-
RA-5	P1	Analyse des vulnérabilités	Gestion
SA - Acquisition des systèmes et des services			
SA-1	P1	Politique et procédures d'acquisition des systèmes et des services	Gestion
SA-2	P1	Affectation des ressources	Gestion
SA-3	P1	Soutien du cycle de vie	Gestion
SA-4	P1	Acquisitions	Gestion
SA-5	P1	Documentation des systèmes d'information	Gestion
SA-6	P1	Restrictions relatives à l'utilisation de logiciel	Gestion
SA-7	P1	Logiciel installé d'utilisateur	Gestion
SA-8	P2	Principes d'ingénierie de la sécurité	Gestion
SA-9	P1	Services de système d'information externes	Gestion
SA-10	P1	Gestion de la configuration par les développeurs	Gestion
SA-11	P1	Tests de sécurité effectués par les développeurs	Gestion
SA-12	P1	Protection de la chaîne d'approvisionnement	Gestion
SA-13	P1	Robustesse (fiabilité)	Gestion
SA-14	P0	Composantes de système d'information essentielles	Gestion
SC - Protection des systèmes et des communications			
SC-1	P1	Politique et procédures de protection des systèmes et des communications	Technique
SC-2	P1	Partitionnement des applications	Technique
SC-3	P1	Isolation des fonctions de sécurité	Technique
SC-4	P1	Information contenue dans les ressources partagées	Technique
SC-5	P1	Protection contre les dénis de service	Technique
SC-6	P0	Priorité des ressources	Technique
SC-7	P1	Protection des frontières	Technique
SC-8	P1	Intégrité des transmissions	Technique
SC-9	P1	Confidentialité des transmissions	Technique

Contrôle n°	Code de priorité	Nom du contrôle	Classe
SC-10	P2	Déconnexion de réseau	Technique
SC-11	P0	Chemin de confiance	Technique
SC-12	P1	Établissement et gestion des clés de chiffrement	Technique
SC-13	P1	Utilisation de la cryptographie	Technique
SC-14	P1	Protection de l'accès public	Technique
SC-15	P1	Dispositifs d'informatique coopérative	Technique
SC-16	P0	Transmission des attributs de sécurité	Technique
SC-17	P1	Certificats d'infrastructure à clé publique	Technique
SC-18	P1	Code mobile	Technique
SC-19	P1	Voix sur IP	Technique
SC-20	P1	Service sécurisé de résolution de nom et (ou) d'adresse (source autorisée)	Technique
SC-21	P1	Service sécurisé de résolution de nom et (ou) d'adresse (résolveur récursif ou cache)	Technique
SC-22	P1	Architecture et fourniture de service de résolution de nom et (ou) d'adresse	Technique
SC-23	P1	Authenticité des sessions	Technique
SC-24	P1	Défaillance dans un état connu	Technique
SC-25	P0	Nœuds légers	Technique
SC-26	P0	Pièges à pirates	Technique
SC-27	P0	Applications indépendantes des systèmes d'exploitation	Technique
SC-28	P1	Protection de l'information inactive	Technique
SC-29	P0	Hétérogénéité	Technique
SC-30	P0	Techniques de virtualisation	Technique
SC-31	P0	Analyse des voies clandestines	Technique
SC-32	P0	Partitionnement des systèmes d'information	Technique
SC-33	P0	Intégrité de la préparation des transmissions	Technique
SC-34	P0	Programmes exécutables non modifiables	Technique
SC-100	P0	Authentification des sources	Technique
SI - Intégrité de l'information et des systèmes			
SI-1	P1	Politique et procédures d'intégrité de l'information et des systèmes	Opérationnelle
SI-2	P1	Correction des lacunes	Opérationnelle
SI-3	P1	Protection contre le code malveillant	Opérationnelle
SI-4	P1	Surveillance des systèmes d'information	Opérationnelle
SI-5	P1	Directives, alertes et avis de sécurité	Opérationnelle
SI-6	P1	Vérification de la fonctionnalité de sécurité	Opérationnelle
SI-7	P1	Intégrité de l'information et du logiciel	Opérationnelle
SI-8	P1	Protection anti-pourriel	Opérationnelle
SI-9	P2	Restrictions relatives à la saisie d'information	Opérationnelle
SI-10	P1	Validation de la saisie d'information	Opérationnelle
SI-11	P2	Traitement des erreurs	Opérationnelle
SI-12	P2	Traitement et conservation des sorties d'information	Opérationnelle

Contrôle n°	Code de priorité	Nom du contrôle	Classe
SI-13	P0	Prévention des pannes prévisibles	Opérationnelle

3. Programmes de sécurité de l'information

Contrôles organisationnels de gestion du programme de sécurité de l'information

La *Politique sur la sécurité du gouvernement* [Référence 1] et les normes correspondantes (*Gestion de la sécurité des technologies de l'information (GSTI)* du SCT [Référence 8], *Directive sur la gestion de la sécurité ministérielle* du SCT [Référence 11], etc.) exigent des organisations qu'elles développent et mettent en œuvre un programme organisationnel de sécurité de l'information et des systèmes d'information à l'appui des opérations et des biens de l'organisation, incluant ceux fournis et gérés par une autre organisation, un entrepreneur, ou en provenance d'une autre source. Les contrôles de gestion des programmes (PM) de sécurité de l'information décrits dans cette section complètent les contrôles de sécurité de la section 4 et mettent l'accent au plan de la sécurité sur les exigences organisationnelles qui sont indépendantes de tout système particulier et essentielles à la gestion des programmes de sécurité de l'information. Les organisations identifient les responsables organisationnels du développement, de la mise en œuvre, de l'évaluation, de l'autorisation et de la surveillance des contrôles de gestion du programme de sécurité. Elles documentent les contrôles de gestion de programme du plan du programme de sécurité. Le plan du programme organisationnel complète les plans de sécurité individuels développés pour chaque système. Ensemble, les plans de sécurité des systèmes d'information individuels et le programme de sécurité de l'information couvrent la totalité des contrôles de sécurité utilisés par l'organisation.

En plus de documenter les contrôles de gestion du programme de sécurité, le plan met à la disposition de l'organisation, dans un dépôt central, un outil qui permet de documenter tous les contrôles de sécurité de la section 4 qui ont été déclarés contrôles communs (c.-à-d., les contrôles hérités des systèmes d'information organisationnels). Les contrôles de gestion et les contrôles communs inclus dans le plan sont mis en œuvre, évalués au niveau de leur efficacité et autorisés par un cadre supérieur de l'organisation qui possède, en matière de gestion des risques, une autorité et une responsabilité identiques ou similaires à celles des agents responsables de l'autorisation des systèmes d'information. Des plans d'action et des jalons sont développés et maintenus pour la gestion du programme et pour les contrôles communs jugés moins efficaces suite à une évaluation. La gestion des programmes de sécurité de l'information et les contrôles communs sont également assujettis aux mêmes exigences de surveillance permanente que les contrôles de sécurité utilisés dans chaque système d'information organisationnel.

Nota

Les organisations doivent mettre en place des contrôles de gestion des programmes de sécurité qui serviront de base à leur programme de sécurité de l'information. La réussite de la mise en œuvre de ces contrôles dépend de celle des contrôles de gestion du programme de l'organisation.

PM-1 PLAN DU PROGRAMME DE SÉCURITÉ DE L'INFORMATION

Contrôle :

(A) L'organisation développe et diffuse un plan du programme organisationnel de sécurité de l'information qui :

(a) Donne un aperçu des exigences du programme et une description des contrôles de gestion des programmes de sécurité et des contrôles communs existants ou prévus pour répondre à ces exigences;

(b) Donne suffisamment d'information sur les contrôles de gestion de programme et les contrôles communs (incluant la spécification explicite ou par référence des paramètres d'affectation et de sélection des contrôles) pour permettre une mise en œuvre formellement conforme à l'objectif du plan ainsi que la détermination subséquente des risques potentiels lorsque le plan est mis en œuvre tel que prévu;

(c) Inclut de l'information sur la conformité, les rôles, les responsabilités, l'engagement de la direction et la coordination entre les entités organisationnelles;

(d) Est approuvé par un cadre supérieur responsable et tenu de rendre compte des risques encourus par les activités (incluant la mission, les fonctions, l'image et la réputation) et les biens de l'organisation, les individus, les autres organisations et le Canada;

(B) L'organisation examine le plan du programme organisationnel de sécurité [*Affectation : fréquence définie par l'organisation*]; et

(C) L'organisation révise le plan pour tenir compte des changements organisationnels et des problèmes identifiés durant la mise en œuvre du plan ou les évaluations des contrôles de sécurité.

Conseils supplémentaires : Le développement du plan du programme de sécurité peut être décrit dans un ou plusieurs documents, à la discrétion de l'organisation. Le plan documente les contrôles de gestion du programme et les contrôles communs définis par l'organisation. Les plans de sécurité des systèmes d'information individuels et le plan du programme organisationnel de sécurité assurent ensemble la totalité des contrôles de sécurité utilisés dans l'organisation. Les contrôles communs sont documentés dans un appendice du plan du programme de sécurité, à moins qu'ils ne soient inclus dans le plan de sécurité d'un système distinct (p. ex., les contrôles de sécurité utilisés dans un système de détection d'intrusion pour la protection, à l'échelle de l'organisation, des frontières héritées d'un ou de plusieurs systèmes). Le plan du programme organisationnel de sécurité indique les plans de sécurité individuels qui incluent les descriptions des contrôles communs.

Les organisations ont le choix de décrire les contrôles communs dans un ou plusieurs documents. Si elles utilisent plusieurs documents, ceux qui décrivent les contrôles communs sont inclus comme pièces jointes au plan du programme de sécurité. Si le plan contient plusieurs documents, l'organisation identifie dans chacun le ou les agents organisationnels responsables du développement, de la mise en œuvre, de l'évaluation, de l'autorisation et de la surveillance de chaque contrôle commun. Par exemple, l'organisation peut exiger que les responsables de la gestion des installations développent, mettent en œuvre, évaluent, autorisent et surveillent en permanence les contrôles communs de protection physique et environnementale de la famille PE lorsque ces contrôles ne sont associés à aucun système particulier mais qu'ils interviennent dans plusieurs d'entre eux. Contrôle connexe : PM-8.

Améliorations du contrôle :

Aucune.

Références :

Politique sur la sécurité du gouvernement du SCT [Référence 1].
Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].

PM-2 AGENT PRINCIPAL DE SÉCURITÉ DE L'INFORMATION

Contrôle :

(A) L'organisation nomme l'agent principal de sécurité de l'information et lui confie, en même temps que les ressources requises, la mission de coordonner, développer, mettre en œuvre et maintenir le programme organisationnel de sécurité de l'information.

Conseils supplémentaires : L'agent de sécurité mentionné dans ce contrôle est l'agent de l'organisation. Dans les organisations fédérales, son rôle est celui d'agent de la sécurité ministérielle. Certaines responsabilités peuvent être déléguées au coordonnateur de la sécurité des TI.

Améliorations du contrôle :

Aucune.

Références :

Politique sur la sécurité du gouvernement du SCT [Référence 1].
Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].
Directive sur la gestion de la sécurité ministérielle du SCT [Référence 11].

PM-3 RESSOURCES LIÉES À LA SÉCURITÉ DE L'INFORMATION

Contrôle :

(A) L'organisation s'assure que toutes les demandes de planification des immobilisations et des investissements incluent les ressources nécessaires à la mise en œuvre du programme de sécurité et documentent toutes les exceptions à cette exigence;

(B) L'organisation effectue une analyse de rentabilisation pour identifier les ressources nécessaires; et

(C) L'organisation s'assure que les ressources liées à la sécurité de l'information peuvent être utilisées tel que prévu.

Conseils supplémentaires : Les organisations peuvent désigner et habiliter un conseil d'examen des programmes (ou un groupe similaire) chargé de gérer et de surveiller les aspects liés à la sécurité de l'information du processus de contrôle de la planification des immobilisations et des investissements. Contrôles connexes : PM-4, SA-2.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

PM-4 PROCESSUS DES PLANS D'ACTION ET JALONS

Contrôle :

(A) L'organisation met en œuvre un processus pour assurer la tenue à jour des plans d'action et des jalons du programme de sécurité et des systèmes d'information organisationnels correspondants et pour documenter les mesures correctives pertinentes d'atténuation des risques qui menacent les activités et les biens de l'organisation, les individus, les autres organisations et le Canada.

Conseils supplémentaires : Le plan d'action et les jalons constituent un document clé du programme de sécurité et sont assujettis aux exigences du SCT en matière de déclaration. Les mises à jour du plan et des jalons s'appuient sur les constatations des évaluations des contrôles de sécurité, les analyses des répercussions sur la sécurité et les activités de surveillance permanente. Le guide du SCT en matière de déclaration inclut des directives concernant les plans d'action et les jalons organisationnels. Contrôle connexe : CA-5.

Améliorations du contrôle :

Aucune.

Références :

Directive sur la gestion de la sécurité ministérielle du SCT [Référence 11].
Guide de gestion des risques de sécurité des systèmes d'information (ITSG-33) du CSTC [Référence 59].

PM-5 INVENTAIRES DES SYSTÈMES D'INFORMATION

Contrôle :

(A) L'organisation développe et tient à jour un inventaire de ses systèmes d'information.

Conseils supplémentaires : Ce contrôle traite des exigences relatives aux inventaires de la *Directive sur la gestion de la sécurité ministérielle* du SCT.

Améliorations du contrôle :

Aucune.

Références :

Directive sur la gestion de la sécurité ministérielle du SCT [Référence 11].

PM-6 MESURES DU RENDEMENT DE LA SÉCURITÉ DE L'INFORMATION

Contrôle :

(A) L'organisation développe et surveille les résultats des mesures du rendement de la sécurité de l'information et produit les rapports pertinents.

Conseils supplémentaires : Les mesures sont des paramètres basés sur des résultats que l'organisation utilise pour mesurer l'efficacité et l'efficience du programme de sécurité et de ses contrôles.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

PM-7 ARCHITECTURE D'ENTREPRISE

Contrôle :

(A) L'organisation développe une architecture d'entreprise en tenant compte de la sécurité de l'information et des risques qui menacent les activités et les biens de l'organisation, les individus, les autres organisations et le Canada.

Conseils supplémentaires : L'intégration des exigences de sécurité et des contrôles correspondants à l'architecture d'entreprise de l'organisation permet de s'assurer que les aspects liés à la sécurité sont pris en compte par l'organisation dès les premiers stades du cycle de développement des systèmes et qu'ils sont directement et explicitement associés à sa mission et à ses processus opérationnels. En plus, cette approche permet d'intégrer à l'architecture d'entreprise une architecture de sécurité intégrale conforme aux stratégies organisationnelles de sécurité et de gestion du risque. Le cadre de gestion du risque et les normes et lignes directrices pertinentes en matière de sécurité permettent de réaliser une intégration efficace des exigences et des contrôles. Contrôles connexes : PL-2, PM-11, RA-2.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

PM-8 PLAN DE L'INFRASTRUCTURE ESSENTIELLE

Contrôle :

(A) L'organisation tient compte des aspects liés à la sécurité de l'information durant le développement, la documentation et la mise à jour du plan de protection de l'infrastructure essentielle et des ressources clés.

Conseils supplémentaires : Les exigences et les directives concernant la définition de l'infrastructure essentielle et des ressources clés et la préparation d'un plan correspondant de protection de l'infrastructure sont définies dans les politiques, normes et procédures pertinentes du GC. Contrôles connexes : PM-1, PM-9, PM-11, RA-3.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

PM-9 STRATÉGIE DE GESTION DU RISQUE

Contrôle :

(A) L'organisation développe une stratégie détaillée de gestion des risques liés à l'exploitation et à l'utilisation des systèmes d'information et qui menacent les activités et les biens de l'organisation, les individus, les autres organisations et le Canada; et

(B) L'organisation applique la stratégie de manière uniforme à l'échelle de l'organisation.

Conseils supplémentaires : Une stratégie organisationnelle de gestion du risque inclut, par exemple, une expression formelle de la tolérance au risque de l'organisation, des méthodologies acceptables d'évaluation des

risques, des stratégies d'atténuation, un processus organisationnel d'évaluation uniforme des risques qui tient compte de la tolérance au risque de l'organisation, et des approches de surveillance permanente des risques. La nomination d'un gestionnaire responsable des aspects liés aux risques peut faciliter l'application uniforme de la stratégie de gestion du risque à l'échelle de l'organisation. La stratégie organisationnelle de gestion peut bénéficier des renseignements sur les risques obtenus d'autres sources tant internes qu'externes et ainsi confirmer son caractère général et exhaustif. Contrôle connexe : RA-3.

Améliorations du contrôle :

Aucune.

Références :

Guide de gestion des risques de sécurité des systèmes d'information (ITSG-33) du CSTC [Référence 59].

PM-10 PROCESSUS D'AUTORISATION DE SÉCURITÉ

Contrôle :

(A) L'organisation gère (c.-à-d., documente, assure le suivi et produit des rapports) la situation des systèmes d'information organisationnels au plan de la sécurité en recourant à un processus d'autorisation de sécurité;

(B) L'organisation attribue à des individus des rôles et responsabilités spécifiques dans son processus de gestion du risque ; et

(C) L'organisation intègre l'ensemble du processus d'autorisation de sécurité à son programme de gestion du risque.

Conseils supplémentaires : Le processus d'autorisation de sécurité pour les systèmes d'information exige la mise en œuvre du cadre de gestion du risque et l'application des normes et lignes directrices de sécurité correspondantes. Les rôles spécifiques que joue le processus de gestion du risque incluent la désignation d'un agent d'autorisation pour chaque système d'information organisationnel. Contrôle connexe : CA-6.

Améliorations du contrôle :

Aucune.

Références :

Guide de gestion des risques de sécurité des systèmes d'information (ITSG-33) du CSTC [Référence 59].

PM-11 DÉFINITION DES PROCESSUS LIÉS À LA MISSION ET AUX OPÉRATIONS

Contrôle :

(A) L'organisation définit les processus liés à la mission et aux opérations en tenant compte de la sécurité de l'information et des risques qui menacent les activités organisationnelles, les biens de l'organisation, les individus, les autres organisations et le Canada; et

(B) L'organisation détermine les besoins de protection de l'information découlant de la définition des processus liés à la mission et aux opérations et, au besoin, révise les processus jusqu'à l'obtention d'un ensemble réalisable d'exigences.

Conseils supplémentaires : Les besoins de protection de l'information s'appuient sur des capacités indépendantes de la technologie et nécessaires pour contrer les risques de compromission de l'information (c.-à-d., perte de confidentialité, d'intégrité ou de disponibilité) qui menacent les organisations, les individus ou

le Canada. Ils découlent de la mission et des besoins opérationnels définis par l'organisation, des processus (liés à la mission et aux opérations) sélectionnés pour répondre aux besoins énoncés et de la stratégie organisationnelle de gestion du risque. Ils déterminent les contrôles de sécurité requis par l'organisation et les systèmes d'information qui exécutent les processus liés à la mission et aux opérations. Une bonne compréhension du niveau potentiel d'incidence négative des risques de compromission de l'information est inhérente à la définition des exigences de protection de l'information de l'organisation. Le processus de catégorisation de la sécurité sert à déterminer de telles incidences potentielles. L'organisation doit documenter les définitions des processus liés à la mission et aux opérations et les exigences de protection de l'information correspondantes, conformément à la politique et aux procédures organisationnelles. Contrôles connexes : PM-7, PM-8, RA-2.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

4. Définitions des contrôles de sécurité

Cette section inclut les définitions des contrôles de sécurité.

Les contrôles de sécurité inclus dans le catalogue sont susceptibles de changer au fil du temps au fur et à mesure que des contrôles sont annulés, révisés ou ajoutés. Aux fins d'assurer la stabilité des plans de sécurité et des outils automatisés de mise en œuvre, nous ne renumérotons pas les contrôles de sécurité et les améliorations de contrôle chaque fois qu'un contrôle et (ou) une amélioration sont annulés. Les numéros seront conservés dans le catalogue à des fins historiques.

Nota

Ce catalogue a été créé comme outil pour faciliter le travail des praticiens de la sécurité chargés de la protection de l'information et des systèmes d'information, en conformité avec les lois pertinentes du GC et les politiques, directives et normes du SCT. Toutefois, dans l'éventualité d'écarts ou de conflits entre les contrôles de sécurité définis dans le catalogue et les lois et politiques du GC ainsi que les politiques, directives et normes du SCT, ces dernières ont préséance.

4.1 FAMILLE : CONTRÔLE D'ACCÈS

CLASSE : TECHNIQUE

AC-1 POLITIQUE ET PROCÉDURES DE CONTRÔLE D'ACCÈS

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique de contrôle d'accès formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de contrôle d'accès et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles d'accès. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique de contrôle d'accès peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures de contrôle d'accès peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique de contrôle d'accès. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].

AC-2 GESTION DES COMPTES

Contrôle :

L'organisation assure la gestion des comptes de système d'information, incluant :

(A) L'identification des types de compte (c.-à-d., comptes individuels, de groupe, de système, d'application, d'invités/anonymes et temporaires).

(B) L'établissement des conditions d'appartenance à un groupe.

(C) L'identification des utilisateurs autorisés et l'établissement des privilèges d'accès.

(D) L'exigence d'approbations appropriées pour les demandes d'établissement des comptes.

(E) L'établissement, l'activation, la modification, la désactivation et la suppression de comptes.

(F) L'autorisation et la surveillance spécifiques de l'utilisation des comptes d'invités/anonymes et temporaires.

(G) Le signalement, aux gestionnaires de comptes, des comptes temporaires qui ne sont plus requis, du départ ou du transfert d'utilisateurs, ou des changements apportés à l'utilisation du système ou au besoin de connaître et (ou) de partager l'information.

(H) La désactivation (i) des comptes temporaires qui ne sont plus requis et (ii) des comptes d'utilisateurs transférés qui ont quitté le GC.

(I) L'octroi de droit d'accès au système basé sur (i) une autorisation d'accès valable, (ii) une utilisation prévue et (iii) d'autres attributs exigés par l'organisation ou associés à des fonctions liées à la mission et (ou) aux opérations.

(J) L'examen des comptes [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : L'identification des utilisateurs autorisés du système et la spécification des privilèges d'accès sont conformes aux exigences des autres contrôles de sécurité du plan de sécurité. Les utilisateurs qui ont besoin de privilèges administratifs pour accéder aux comptes sont soumis à un examen minutieux supplémentaire de la part des agents de l'organisation responsables de l'approbation de ces types de compte et de l'accès privilégié. Contrôles connexes : AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-4, IA-5, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour appuyer la gestion des comptes de système.

(2) Le système annule automatiquement les comptes temporaires et d'urgence après [*Affectation : durée définie par l'organisation pour chaque type de compte*].

(3) Le système désactive automatiquement les comptes inactifs après [*Affectation : durée définie par l'organisation*].

(4) Le système vérifie automatiquement la création, la modification et la désactivation des comptes et les actions de cessation d'emploi, et en informe les personnes concernées, le cas échéant.

(5) L'organisation :

(a) Exige des utilisateurs qu'ils se déconnectent après [*Affectation : durée d'inactivité prévue et (ou) description du moment de la déconnexion définies par l'organisation*];

(b) Détermine la durée d'utilisation (incluant l'heure de la journée) des comptes;

(c) Surveille toute utilisation atypique des comptes; et

(d) Signale toute utilisation atypique aux agents désignés de l'organisation.

(6) Le système gère de manière dynamique les privilèges d'utilisateur et les autorisations d'accès correspondantes.

Conseils supplémentaires d'amélioration : Contrairement aux approches conventionnelles du contrôle d'accès qui utilisent l'information statique sur les comptes et des ensembles prédéfinis de privilèges d'utilisateur, plusieurs versions d'architectures axées sur les services misent sur des décisions de contrôles d'accès prises en temps réel et facilitées par une gestion dynamique des privilèges. Les identités d'utilisateur demeurent relativement constantes au fil du temps; toutefois, les privilèges peuvent changer plus fréquemment selon les exigences de la mission et les besoins opérationnels de l'organisation.

(7) L'organisation :

(a) Établit et administre les comptes d'utilisateur privilégiés en conformité avec un schéma d'accès axé sur les rôles qui définit sous forme de rôles les privilèges associés au système et au réseau; et

(b) Piste et surveille les attributions de rôles privilégiés.

Conseils supplémentaires d'amélioration : Les rôles privilégiés incluent, par exemple, la gestion des clés, l'administration du réseau et du système et l'administration des bases de données et du Web.

Références :

Aucune.

AC-3 APPLICATION DES DROITS D'ACCÈS

Contrôle :

(A) Le système d'information applique les autorisations d'accès logique approuvées en conformité avec la politique concernée.

Conseils supplémentaires : Les politiques de contrôle d'accès (p. ex., politiques axées sur l'identité, sur les rôles et sur les attributs) et les mécanismes d'application des droits d'accès (listes de contrôle d'accès, matrices de contrôle d'accès, cryptographie, etc.) sont utilisés par les organisations pour contrôler l'accès entre les utilisateurs (ou les processus exécutés en leur nom) et les objets (dispositifs, fichiers, dossiers, processus, programmes, domaines, etc.) dans le système d'information. En plus de permettre l'accès au niveau du système, les mécanismes d'application des droits d'accès sont utilisés au niveau de l'application, le cas échéant, pour accroître la sécurité de l'information. On doit envisager le recours à une fonction explicite et vérifiée de contournement des mécanismes automatisés en cas d'urgence et dans l'éventualité d'événements graves. Si le mécanisme d'application des droits d'accès chiffre l'information stockée, la cryptographie utilisée doit être conforme aux exigences du contrôle SC-13. Dans le cas de l'information classifiée, la cryptographie choisie est intimement liée au niveau de classification de l'information et aux cotes de sécurité des personnes qui y ont accès. Les mécanismes prévus dans le contrôle AC-3 sont configurés de manière à appliquer les autorisations définies par d'autres contrôles de sécurité. Contrôles connexes : AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Améliorations du contrôle :

(1) [Annulée : Intégrée au contrôle AC-6].

(2) Le système applique une double autorisation basée sur les politiques et procédures organisationnelles concernant [*Affectation : commandes privilégiées définies par l'organisation*].

Conseils supplémentaires d'amélioration : Les mécanismes de double autorisation exigent l'exécution de deux formes d'approbation. L'organisation ne recoure pas à ces mécanismes lorsqu'il faut intervenir dans les plus brefs délais pour assurer la sécurité publique et environnementale.

(3) Le système applique [*Affectation : politiques de contrôle d'accès non discrétionnaires définies par l'organisation]* aux *[Affectation : ensembles d'utilisateurs et de ressources définis par l'organisation*] lorsque l'ensemble de règles de chaque politique précise :

(a) L'information sur le contrôle d'accès (c.-à-d., attributs) qu'il utilise (p. ex., poste, nationalité, âge, projet, heure du jour); et

(b) Les relations obligatoires entre les renseignements de contrôle d'accès pour autoriser l'accès.

Conseils supplémentaires d'amélioration : Les politiques non discrétionnaires de contrôle d'accès que les organisations peuvent utiliser incluent, par exemple, le contrôle d'accès axé sur les attributs, le contrôle d'accès obligatoire et le contrôle d'accès géré par le demandeur. Les organisations peuvent utiliser ces politiques en plus des politiques discrétionnaires.

Contrôle d'accès obligatoire (MAC) : La politique définit tous les sujets et objets qu'elle contrôle afin de s'assurer que chaque utilisateur reçoit uniquement l'information à laquelle il est autorisé à accéder selon la classification de l'information et la cote de sécurité et l'autorisation formelle d'accès qu'il détient. Le système assigne les attributs de sécurité appropriés (p. ex., étiquettes, domaines de sécurité, types) aux sujets et aux objets et utilise ces attributs comme base des décisions MAC. Le modèle de sécurité Bell-LaPadula définit l'accès autorisé en tenant compte d'un ensemble de niveaux de sécurité hiérarchiques stricts définis par l'organisation : un sujet peut lire un objet seulement si son niveau de sécurité est supérieur à celui de l'objet et peut écrire dans un objet seulement si les deux conditions suivantes sont satisfaites : le niveau de sécurité de l'objet est supérieur à celui du sujet et le niveau de la cote de sécurité de l'utilisateur est supérieur au niveau de sécurité de l'objet.

Contrôles d'accès axés sur les rôles (CAAR) : La politique définit tous les utilisateurs et toutes les ressources qu'elle contrôle afin de s'assurer que les droits d'accès sont groupés par nom de rôle et que l'accès aux ressources est réservé aux utilisateurs qui ont été autorisés à remplir ce rôle.

(4) Le système applique une politique de contrôle d'accès discrétionnaire (DAC) qui :

(a) Permet aux utilisateurs de préciser et de contrôler le partage d'information soit avec des individus ou des groupes d'individus identifiés, ou les deux;

(b) Limite la propagation des droits d'accès; et

(c) Inclut ou exclut l'accès à la granularité d'un seul utilisateur.

(5) Le système empêche l'accès à [*Affectation : information de sécurité définie par l'organisation*] sauf durant les états de non fonctionnement et sécurisés du système.

Conseils supplémentaires d'amélioration : L'information sur la sécurité est toute information susceptible d'influer sur l'exécution des fonctions de sécurité de manière à nuire à l'application de la politique de sécurité du système ou à isoler le code et les données. Les exemples d'information sur la sécurité incluent les règles de filtrage des routeurs et pare-feu, l'information de gestion des clés de chiffrement, les paramètres clés de configuration des services de sécurité et les listes de contrôle d'accès. Les états de non fonctionnement et sécurisés du système sont des états pendant lesquels le système n'effectue aucun traitement lié à la mission et (ou) aux opérations (p. ex., système hors ligne aux fins de maintenance, de dépannage, d'amorçage ou d'arrêt).

(6) L'organisation chiffre ou conserve hors ligne dans un endroit protégé [*Affectation : information sur l'utilisateur et (ou) le système définie par l'organisation*].

Conseils supplémentaires d'amélioration : L'utilisation du chiffrement réduit la probabilité de divulgation non autorisée d'information et peut également détecter les modifications non autorisées. Le transfert de l'information stockée en ligne vers un dispositif de stockage hors ligne élimine la possibilité que des individus puissent accéder à l'information de manière non autorisée par un réseau. Contrôle connexe : MP-4.

Références :

Aucune.

AC-4 APPLICATION DES CONTRÔLES DE FLUX D'INFORMATION

Contrôle :

(A) Le système d'information recoure à des autorisations formelles de contrôle des flux d'information dans le système et entre les systèmes interconnectés, en conformité avec la politique concernée.

Conseils supplémentaires : Le contrôle du flux d'information régit le cheminement de l'information dans un système et entre des systèmes (par opposition aux personnes autorisées à y accéder), quels que soient les accès subséquents à cette information. Les exemples de restrictions de contrôle de flux incluent les suivants : empêcher l'information contrôlée à des fins d'exportation de transiter en clair dans Internet, bloquer le trafic entrant qui prétend provenir de l'intérieur de l'organisation et ne pas transmettre dans Internet de demandes Web qui ne proviennent pas du mandataire Web interne. Les organisations utilisent couramment les politiques et les mécanismes d'application des contrôles de flux d'information pour contrôler le flux entre des sources et des destinations précises (p. ex., réseaux, individus, dispositifs) dans les systèmes individuels et entre les systèmes interconnectés. Le contrôle de flux est lié aux caractéristiques de l'information et (ou) à ses voies de communication. On peut trouver des exemples types de ces contrôles dans les dispositifs de protection des frontières (p. ex., mandataires, passerelles, agents de sécurité, tunnels chiffrés, pare-feu et routeurs); ceux-ci utilisent des ensembles de règles ou établissent des paramètres de configuration qui limitent les services du système et offrent une capacité de filtrage de paquets basée sur l'information d'en-tête ou une capacité de filtrage de messages basée sur le contenu (p. ex., en utilisant des recherches de mots clés ou les caractéristiques d'un document). Les mécanismes appliqués par le contrôle AC-4 sont configurés de manière à tenir compte des autorisations définies par d'autres contrôles de sécurité. Contrôles connexes : AC-17, AC-19, AC-21, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Améliorations du contrôle :

(1) Le système applique le contrôle de flux d'information en utilisant des attributs de sécurité explicites, pour l'information et les objets source et de destination, comme base pour les décisions concernant le contrôle de flux.

Conseils supplémentaires d'amélioration : Les mécanismes d'application de flux d'information comparent les attributs de sécurité de l'ensemble de l'information (contenu et structure des données) et des objets source et de destination et interviennent de manière appropriée (p. ex., blocage, mise en quarantaine, avertissement de l'administrateur) lorsqu'ils identifient des flux d'information non explicitement autorisés par la politique sur le flux d'information. L'application du contrôle de flux d'information basée sur des attributs de sécurité peut servir, par exemple, à contrôler la diffusion de certains types d'information.

(2) Le système applique le contrôle de flux d'information en utilisant des domaines de traitement protégés (p. ex., application de type de domaine) comme base pour les décisions concernant le contrôle de flux.

(3) Le système applique le contrôle dynamique de flux d'information en s'appuyant sur une politique qui permet ou interdit les flux d'information en fonction de conditions changeantes ou de motifs opérationnels.

(4) Le système empêche les données chiffrées de contourner les mécanismes de vérification de contenu.

(5) Le système applique [*Affectation : restrictions définies par l'organisation concernant l'intégration de types de données dans d'autres types de données*].

(6) Le système applique le contrôle de flux d'information aux métadonnées.

(7) Le système applique [*Affectation : flux unidirectionnels définis par l'organisation*] en utilisant des mécanismes matériels.

(8) Le système applique le contrôle de flux d'information en utilisant [*Affectation : filtres de la politique de sécurité définis par l'organisation*] comme base pour les décisions concernant le contrôle de flux.

Conseils supplémentaires d'amélioration : Les filtres de la politique de sécurité définis par l'organisation incluent, par exemple, les filtres de mots à proscrire, de type de fichier, de données structurées et non structurées, de contenu des métadonnées et de contenu caché. Les données structurées permettent l'interprétation de leur contenu en raison des éléments atomiques indivisibles qu'une application est en mesure de comprendre. Les données non structurées désignent la masse d'information (habituellement) numérique sans structure ou dont la structure ne peut être facilement lue par une machine. Elles comprennent deux catégories de base : (i) tables de bits, essentiellement indépendantes de tout langage (c.-à-d., fichiers d'images, vidéo ou audio); et (ii) objets textuels associés à un langage d'écriture ou d'impression (c.-à-d., documents de systèmes de traitement de texte commerciaux standard, tableurs ou courriels).

(9) Le système recoure à une vérification manuelle de [*Affectation : filtres de la politique de sécurité définis par l'organisation*] lorsqu'il n'est pas en mesure de prendre de décision concernant le contrôle de flux d'information.

(10) Le système permet à un administrateur privilégié d'activer/désactiver [*Affectation : filtres de la politique de sécurité définis par l'organisation*].

(11) Le système permet à un administrateur privilégié de configurer [*Affectation : filtres de la politique de sécurité définis par l'organisation*] pour appuyer les différentes politiques de sécurité.

Conseils supplémentaires d'amélioration : Par exemple, pour refléter les modifications apportées à la politique de sécurité, un administrateur peut changer la liste des mots à proscrire vérifiée par les mécanismes de la politique, en conformité avec les définitions fournies par l'organisation.

(12) Le système, lors du transfert d'information entre différents domaines de sécurité, identifie les flux d'information selon la spécification du type de données et l'utilisation des données.

Conseils supplémentaires d'amélioration : La spécification du type de données et l'utilisation des données incluent, par exemple, l'attribution de noms de fichier qui reflètent le type de données et la restriction des transferts de données selon le type de fichier.

(13) Le système, lors du transfert d'information entre différents domaines de sécurité, décompose l'information en sous-composantes pour la présenter aux mécanismes d'application de la politique.

Conseils supplémentaires d'amélioration : Les mécanismes d'application de la politique incluent les règles de filtrage et (ou) de nettoyage appliquées à l'information avant son transfert à un domaine de sécurité différent. L'analyse syntaxique des fichiers de transfert facilite les décisions de nature politique concernant la source, la destination, les certificats, la classification, le sujet, les pièces jointes et autres différenciateurs de composantes liées à la sécurité de l'information. Les règles de politique concernant les transferts entre domaines incluent, par exemple, les restrictions d'insertion de types de composante et (ou) d'information dans d'autres types de même nature, l'interdiction d'utiliser plus de deux niveaux d'insertion et l'interdiction du transfert de types d'information archivée.

(14) Le système, lors du transfert d'information entre différents domaines de sécurité, applique les filtres de la politique qui limitent la structure et le contenu des données selon [*Affectation : exigences de la politique de sécurité de l'information définies par l'organisation*].

Conseils supplémentaires d'amélioration : L'établissement de contraintes concernant la taille des fichiers, les énumérations permises, les jeux de caractères, les schémas et autres attributs d'objet de données réduit la quantité de contenu potentiellement malveillant et (ou) illicite. Les exemples de contraintes incluent les mesures qui permettent de s'assurer que les champs de caractères incluent uniquement (i) des caractères ASCII imprimables et (ii) des caractères alphanumériques, (iii) n'incluent aucun caractère spécial, ou (iv) que la taille maximale des champs et des fichiers respecte celle stipulée dans la politique de sécurité l'organisation.

(15) Le système, lors du transfert d'information entre différents domaines de sécurité, détecte l'information non autorisée et en interdit le transfert, en conformité avec la politique de sécurité.

Conseils supplémentaires d'amélioration : Les mesures de soutien de cette amélioration incluent la détection de maliciel et la consultation de la liste des mots à proscrire pour l'information transférée, et l'application aux métadonnées des mêmes mesures de protection (p. ex., attributs de sécurité) que celles utilisées pour les paquets d'information.

(16) Le système applique les politiques de sécurité concernant l'information contenue dans les systèmes interconnectés.

Conseils supplémentaires d'amélioration : Le transfert d'information entre des systèmes interconnectés qui utilisent des politiques de sécurité différentes pose des risques de contravention à l'une ou l'autre des nombreuses politiques. Les contraventions aux politiques de sécurité peuvent de pas être absolument interdites. Les propriétaires et (ou) gardiens de l'information appliquent leur politiques à des points précis entre les systèmes interconnectés. On recommande de recourir à des solutions architecturales, le cas échéant, pour réduire la possibilité que certaines vulnérabilités ne soient pas détectées. Ces solutions incluent, par exemple, (i) l'interdiction de transferts d'information entre systèmes interconnectés (c.-à-d., application de mécanismes de transfert unidirectionnels en mode accès seulement), (ii) l'utilisation de mécanismes matériels pour les flux d'information unidirectionnels et (iii) la mise en œuvre de mécanismes remaniés et testés de manière exhaustive pour réassigner les attributs de sécurité et les étiquettes correspondantes.

(17) Le système :

(a) Identifie de façon unique et authentifie les domaines source et de destination pour le transfert d'information;

(b) Relie les attributs de sécurité à l'information pour faciliter l'application de la politique sur le flux d'information; et

(c) Piste les problèmes associés à la liaison aux attributs de sécurité et au transfert d'information.

Conseils supplémentaires d'amélioration : L'attribution est une composante essentielle du concept d'opération de sécurité. La capacité d'identifier les points source et de destination du flux des données dans un système d'information permet, le cas échéant, la reconstruction à des fins judiciaires des événements et accroit le respect des politiques en attribuant les contraventions à des organisations et (ou) des individus spécifiques. Les moyens d'application de cette amélioration incluent les mesures pour s'assurer que les étiquettes produites par le système d'information permettent une distinction entre les systèmes d'information et les organisations et entre les composantes de système ou les individus qui participent à la préparation, l'envoi, la réception ou la diffusion d'information.

Références :

Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22) du CSTC [Référence 42].

AC-5 SÉPARATION DES TÂCHES

Contrôle :

(A) L'organisation procède au besoin à la séparation des tâches des individus pour empêcher toute activité malveillante sans collusion.

(B) L'organisation documente la séparation des tâches.

(C) L'organisation applique la séparation des tâches en attribuant des autorisations d'accès aux systèmes d'information.

Conseils supplémentaires : Les exemples de séparation des tâches incluent (i) la répartition des fonctions liées à la mission et de certaines fonctions de soutien du système d'information entre différents individus et (ou) rôles, (ii) l'attribution à différents individus des fonctions de soutien du système d'information (p. ex., gestion et programmation du système, gestion de la configuration, assurance de la qualité et tests, sécurité du réseau), (iii)

l'interdiction au personnel de sécurité d'administrer à la fois les fonctions de contrôle d'accès et les fonctions de vérification, et (iv) l'attribution de différent comptes d'administrateur aux différents rôles. Les autorisations d'accès définies dans ce contrôle sont appliquées par le contrôle AC-3. Contrôles connexes : AC-3.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

AC-6 PRIVILÈGE MINIMUM

Contrôle :

(A) L'organisation utilise le concept de privilège minimum et accorde un accès autorisé uniquement aux utilisateurs (et aux processus exécutés en leur nom) qui en ont besoin pour accomplir les tâches qui leur ont été assignées en conformité avec les missions et les fonctions opérationnelles de l'organisation.

Conseils supplémentaires : Les autorisations d'accès définies ici relèvent dans une large mesure du contrôle AC-3. L'organisation utilise le concept de privilège minimum pour des tâches et des systèmes d'information spécifiques (incluant des ports, protocoles et services particuliers) après avoir effectué, au besoin, des évaluations pour atténuer de façon adéquate les risques qui menacent les activités et les biens de l'organisation, les individus, les autres organisations et le Canada. Contrôles connexes : AC-2, AC-3, CM-7.

Améliorations du contrôle :

(1) L'organisation autorise l'accès explicitement aux [*Affectation : liste définie par l'organisation des fonctions de sécurité (déployées dans le matériel, le logiciel et le micrologiciel) et information sur la sécurité*].

Conseils supplémentaires d'amélioration : L'établissement des comptes système, la configuration des autorisations d'accès (c.-à-d., permissions, privilèges), la définition des événements à vérifier et des paramètres de détection d'intrusion sont des exemples de fonctions de sécurité. Le personnel explicitement autorisé inclut, par exemple, les administrateurs de la sécurité, les administrateurs de système et de réseau, les agents de sécurité de système, le personnel de maintenance de système, les programmeurs de système et autres utilisateurs privilégiés. Contrôle connexe : AC-17.

(2) L'organisation exige des utilisateurs de comptes ou de rôles de système d'information, qui ont accès aux [*Affectation : liste définie par l'organisation des fonctions de sécurité et information sur la sécurité*], qu'ils utilisent des comptes ou des rôles non privilégiés pour accéder aux autres fonctions de système et, dans la mesure du possible, vérifient toute utilisation de comptes ou de rôles privilégiés pour ces fonctions.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle vise à limiter les possibilités d'utilisation des systèmes avec un compte ou un rôle privilégié. Nous avons inclus le *rôle* pour tenir compte des situations de mise en œuvre d'une politique de contrôle d'accès, tel le CAAR, et des situations où la modification d'un rôle entraîne automatiquement la modification des autorisations d'accès de l'utilisateur, et de tous les processus exécutés en son nom, comme ce serait le cas si l'on remplaçait un compte privilégié par un compte non privilégié. La vérification des activités privilégiées peut nécessiter de recourir à des systèmes pour lesquels l''utilisateur ne possède pas d'accès privilégié.

(3) L'organisation autorise l'accès réseau aux [*Affectation : commandes privilégiées définies par l'organisation*] seulement en cas de besoins opérationnels urgents et documente les motifs d'un tel accès dans le plan de sécurité des opérations du système d'information.

(4) Le système fournit des domaines de traitement séparés pour permettre une meilleure granularité lors de l'attribution des privilèges d'utilisateur.

Conseils supplémentaires d'amélioration : L'utilisation de techniques de virtualisation pour permettre davantage de privilèges dans une machine virtuelle, tout en limitant ceux accordés à la machine réelle sous-jacente, est un exemple de recours à des domaines de traitement séparés pour permettre une meilleure granularité lors de l'attribution des privilèges d'utilisateur.

(5) L'organisation limite au personnel d'administration de système désigné l'autorisation d'utiliser les comptes de super utilisateur du système d'information.

Conseils supplémentaires d'amélioration : Les comptes de super utilisateur sont normalement décrits comme des comptes « racines » ou d'« administrateur » dans les différents types de systèmes d'exploitation commerciaux standard. La configuration des systèmes d'information (p. ex., portables, serveurs, postes de travail) de manière à interdire aux utilisateurs normaux tout accès autorisé aux comptes de super utilisateur est un exemple de restriction des autorisations système. Lorsqu'elle applique cette amélioration de contrôle, l'organisation peut faire la différence entre l'attribution de privilèges autorisés aux comptes du système d'information local et aux comptes de domaine pour autant qu'elle garde le contrôle de la configuration du système pour ce qui touche les paramètres clés de sécurité et, le cas échéant, pour assurer une atténuation suffisante des risques.

(6) L'organisation interdit tout accès privilégié au système d'information aux utilisateurs non organisationnels.

Références :

Aucune.

AC-7 TENTATIVES DE CONNEXION NON RÉUSSIES

Contrôle :

(A) Le système d'information applique une limite de [*Affectation : nombre défini par l'organisation*] tentatives de connexion infructueuses consécutives par l'utilisateur sur une période de [*Affectation : durée définie par l'organisation*].

(B) Le système d'information [*Sélection : verrouille le compte et (ou) le nœud pendant [Affectation : durée définie par l'organisation]; verrouille le compte et (ou) le nœud jusqu'à ce qu'un administrateur le libère; reporte le message de connexion suivant à [Affectation : algorithme de temporisation défini par l'organisation]*] automatiquement lorsque le nombre maximal de tentatives infructueuses est dépassé. Le contrôle s'applique tant à une connexion locale qu'à une connexion réseau.

Conseils supplémentaires : En raison des risques de déni de service, les verrouillages automatiques effectués par le système d'information sont habituellement temporaires et annulés automatiquement après une période prédéterminée établie par l'organisation. Dans le cas où on choisit un algorithme de temporisation, l'organisation peut utiliser différents algorithmes pour les différentes composantes de système, selon leurs capacités. La réponse aux tentatives de connexion non réussies peut provenir tant du système d'exploitation que des applications. Ce contrôle s'applique à tous les accès autres que ceux explicitement identifiés et documentés par l'organisation dans le contrôle AC-14.

Améliorations du contrôle :

(1) Le système verrouille automatiquement le compte et (ou) nœud jusqu'à ce qu'il soit libéré par un administrateur lorsque le nombre maximal de tentatives infructueuses est dépassé.

(2) Le système inclut une protection supplémentaire pour les accès par connexion aux dispositifs mobiles; il nettoie l'information après [*Affectation : nombre défini par l'organisation*] tentatives consécutives de connexion infructueuses au dispositif.

Conseils supplémentaires d'amélioration : Cette amélioration s'applique seulement aux dispositifs mobiles (p. ex., assistants numériques) auxquels l'accès se fait par une connexion et non aux autres dispositifs mobiles, tels les supports amovibles. Dans certaines situations, l'amélioration peut ne pas s'appliquer aux dispositifs mobiles lorsque l'information qu'ils contiennent est chiffrée avec des mécanismes de chiffrement suffisamment forts pour qu'on puisse annuler l'opération de nettoyage. La connexion concerne le dispositif mobile lui-même et non l'un de ses comptes. Une connexion réussie à l'un ou l'autre des comptes du dispositif mobile remet à zéro le compteur de connexions infructueuses.

Références :

Aucune.

AC-8 AVIS CONCERNANT L'UTILISATION DU SYSTÈME

Contrôle :

(A) Le système d'information, avant d'accorder l'accès, affiche un message approuvé ou une bannière d'avis concernant l'utilisation du système, qui inclut des avis de confidentialité et de sécurité en conformité avec la *Politique d'utilisation des réseaux électroniques du SCT* [Référence 6].

(B) Le système d'information maintient l'affichage du message ou de la bannière d'avis jusqu'à ce que les utilisateurs décident de se connecter ou d'accéder au système.

(C) Le système d'information, dans le cas d'un système accessible au public, (i) affiche, le cas échéant, l'information d'utilisation avant d'accorder l'accès, (ii) affiche les mises en garde appropriées conformes aux dispositions sur la confidentialité s'il interdit les activités de surveillance, d'enregistrement ou de vérification et (iii) inclut dans l'avis aux utilisateurs publics du système une description de l'utilisation autorisée du système.

Conseils supplémentaires : Les messages d'avis concernant l'utilisation du système peuvent prendre la forme de bannières d'avertissement qui s'affichent lorsque les utilisateurs se connectent au système. L'avis concerne uniquement les accès d'utilisateur humain effectués par une interface de connexion et ne s'affiche pas lorsqu'une telle interface n'existe pas.

Améliorations du contrôle :

Aucune.

Références :

Politique d'utilisation des réseaux électroniques du SCT [Référence 6].

AC-9 AVIS CONCERNANT LES CONNEXION ANTÉRIEURES (ACCÈS)

Contrôle :

(A) Le système d'information indique à l'utilisateur qui a réussi à se connecter la date et l'heure de sa dernière connexion (dernier accès).

Conseils supplémentaires : Le but de ce contrôle est de tenir compte à la fois des connexions traditionnelles aux systèmes d'information et de l'accès général à ces systèmes offert par d'autres types de configuration architecturale (p. ex., architectures axées sur les services).

Améliorations du contrôle :

(1) Le système indique à l'utilisateur qui a réussi à se connecter le nombre de tentatives de connexions infructueuses depuis sa dernière connexion réussie

(2) Le système indique à l'utilisateur le nombre de [*Sélection : connexions/accès réussies; connexions/accès non réussies; les deux*] pendant [*Affectation : durée définie par l'organisation*].

(3) Le système informe l'utilisateur de [*Affectation : ensemble de modifications, défini par l'organisation, liées à la sécurité et apportées au compte de l'utilisateur]* pendant *[Affectation : durée définie par l'organisation*].

Références :

Aucune.

AC-10 CONTRÔLE DES SESSIONS SIMULTANÉES

Contrôle :

(A) Le système d'information limite le nombre de sessions simultanées de chaque compte système à [*Affectation : nombre défini par l'organisation*]

Conseils supplémentaires : L'organisation peut définir globalement le nombre maximal de sessions simultanées d'un compte système par type de compte, par compte ou une combinaison de deux. Ce contrôle concerne les sessions simultanées d'un compte système particulier et non celles effectuées par un individu qui utilise plusieurs comptes.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

AC-11 VERROUILLAGE DE SESSION

Contrôle :

(A) Le système d'information empêche tout autre accès au système en verrouillant la session après [*Affectation : durée définie par l'organisation*] d'inactivité ou sur réception d'une demande d'un utilisateur.

(B) Le système d'information maintient le verrouillage de la session jusqu'à ce que l'utilisateur réinitialise l'accès en exécutant les procédures établies d'identification et d'authentification.

Conseils supplémentaires : Un verrouillage de session est une mesure temporaire prise lorsqu'un utilisateur cesse de travailler sur son poste et s'éloigne de l'environnement immédiat où se trouve le système d'information et qu'il ne souhaite pas se déconnecter en raison de la nature temporaire de son absence. Le verrouillage est effectué à un moment où il est possible de déterminer l'activité de la session. Cet arrêt est normalement décidé par le système d'exploitation, mais peut également s'effectuer au niveau de l'application. Le verrouillage ne doit pas se substituer, par exemple, à une déconnexion du système, tel que l'exige l'organisation à la fin de la journée de travail.

Améliorations du contrôle :

(1) Le mécanisme de verrouillage de session du système d'information, lorsqu'il est activé dans un dispositif doté d'un écran, affiche différents motifs visibles qui permettent de cacher ce qui figurait précédemment à l'écran.

Références :

Aucune.

AC-12 FIN DE SESSION

[Annulé : Intégré au contrôle SC-10].

AC-13 SURVEILLANCE ET EXAMEN — CONTRÔLE D'ACCÈS

[Annulé : Intégré au contrôle AC-2 et AU-6].

AC-14 OPÉRATIONS PERMISES SANS IDENTIFICATION NI AUTHENTIFICATION

Contrôle :

(A) L'organisation identifie les opérations spécifiques que l'utilisateur peut exécuter dans le système sans s'identifier ni s'authentifier.

(B) L'organisation documente et explique dans le plan de sécurité des opérations du système la logique sous-jacente qui permet à l'utilisateur d'effectuer des opérations qui ne nécessitent ni identification ni authentification.

Conseils supplémentaires : Ce contrôle vise les situations spécifiques pour lesquelles une organisation détermine qu'il n'y a pas lieu d'appliquer les mécanismes d'identification et d'authentification; toutefois, cela ne signifie pas que de telles situations existent automatiquement pour un système donné. L'organisation peut autoriser un nombre limité de telles opérations (p. ex., des individus qui accèdent à des sites Web publics ou à des systèmes fédéraux accessibles au public). Les organisations peuvent également identifier des opérations qui exigent normalement l'intervention de ces mécanismes et permettre une dérogation dans certaines circonstances (p. ex., situations d'urgences). Cette dérogation peut s'effectuer, par exemple, par un commutateur physique, lisible par logiciel, qui permet de contourner la procédure de connexion et qui est protégé contre toute utilisation accidentelle ou non contrôlée. Ce contrôle ne s'applique pas aux situations pour lesquelles l'identification et l'authentification ont déjà été contrôlées et ne sont pas répétées, mais plutôt à celles pour lesquelles les mécanismes d'identification et (ou) d'authentification n'ont pas encore été appliqués. Contrôles connexes : CP-2, IA-2.

Améliorations du contrôle :

(1) L'organisation permet d'effectuer des opérations sans contrôle d'identification ni d'authentification seulement dans la mesure où cela est nécessaire pour atteindre des objectifs opérationnels ou liés à la mission.

Références :

Aucune.

AC-15 MARQUAGE AUTOMATIQUE

[Annulé : Intégré au contrôle MP-3].

AC-16 ATTRIBUTS DE SÉCURITÉ

Contrôle :

(A) Le système d'information maintient et protège la liaison entre [*Affectation : attributs de sécurité définis par l'organisation*] et l'information pendant qu'elle est stockée, traitée et transmise.

Conseils supplémentaires : Les attributs de sécurité sont des abstractions des propriétés ou des caractéristiques de base d'une entité (p. ex., sujets et objets) qui concernent la protection de l'information. Ils sont normalement associés aux structures de données internes (dossiers, tampons, fichiers, etc.) du système; ils permettent d'appliquer les politiques de contrôle d'accès et de flux, énoncent les instructions spéciales de diffusion, de traitement ou de distribution, ou soutiennent d'autres aspects de la politique de sécurité de l'information. Le terme étiquette de sécurité est souvent utilisé pour associer un ensemble d'attributs de sécurité à un objet d'information particulier dans la structure de données de l'objet (p. ex., privilèges d'accès, nationalité, affiliation comme entrepreneur d'un utilisateur). Contrôles connexes : AC-3, AC-4, SC-16, MP-3.

Améliorations du contrôle :

(1) Le système reconfigure de manière dynamique les attributs de sécurité en conformité avec une politique de sécurité désignée au moment de la création et de la combinaison de l'information.

(2) Le système permet aux entités autorisées de modifier les attributs de sécurité.

(3) Le système maintient entre les attributs de sécurité et l'information une liaison à ce point fiable que l'association information-attribut peut servir de base aux opérations automatisées.

Conseils supplémentaires d'amélioration : Les exemples d'opérations automatisées incluent les décisions automatisées de contrôle d'accès (p. ex., décisions concernant le contrôle d'accès obligatoire), ou les décisions de diffuser (ou non) l'information (p. ex., flux d'information entre des systèmes fonctionnant dans plusieurs domaines).

(4) Le système permet aux utilisateurs autorisés d'associer des attributs de sécurité à l'information.

Conseils supplémentaires d'amélioration : Le soutien du système à cet égard peut varier entre inviter les utilisateurs à sélectionner les attributs de sécurité associés à des objets d'information particuliers, et veiller à ce que la combinaison d'attributs sélectionnés soit valable.

(5) Le système affiche sous forme lisible les attributs de sécurité de chaque objet transmis du système à ses dispositifs de sortie afin d'identifier [*Affectation : ensemble d'instructions spéciales de diffusion, de traitement ou de distribution définies par l'organisation*] conformément [*Affectation : conventions d'attribution de noms standard en langage lisible définies par l'organisation*].

Conseils supplémentaires d'amélioration : Les objets de sortie du système d'information incluent, par exemple, des pages, des écrans, ou des objets équivalents. Les dispositifs de sortie incluent, par exemple, les imprimantes et les affichages vidéo sur les terminaux d'ordinateur, les moniteurs, les écrans de portables et les assistants numériques.

Références :

Aucune.

AC-17 ACCÈS À DISTANCE

Contrôle :

(A) L'organisation documente les méthodes autorisées d'accès à distance du système d'information.

(B) L'organisation définit les restrictions d'utilisation et les directives de mise en œuvre de chaque méthode d'accès à distance autorisée.

(C) L'organisation surveille les accès à distance non autorisés du système d'information.

(D) L'organisation autorise l'accès à distance du système d'information avant la connexion.

(E) L'organisation applique les exigences concernant les connexions à distance du système d'information.

(AA) L'organisation s'assure que tous les employés qui travaillent à l'extérieur des locaux protègent l'information conformément aux exigences minimales de la *Norme opérationnelle sur la sécurité matérielle du SCT* [Référence 7].

Conseils supplémentaires : Ce contrôle exige une autorisation explicite, sans en préciser le format, avant de permettre l'accès à distance d'un système d'information. Par exemple, bien que l'organisation puisse juger appropriée l'utilisation d'une entente d'interconnexion de système pour autoriser un accès à distance, le contrôle n'exige pas de telles ententes. Un accès à distance est tout accès par un réseau externe (p. ex., Internet) à un système organisationnel effectué par un utilisateur (ou un processus exécuté en son nom). Exemples de méthodes d'accès à distance : liaison commutée, à large bande et sans fil (voir le contrôle AC-18 pour l'accès sans fil). Un réseau privé virtuel, doté des contrôles de sécurité appropriés, est considéré comme un réseau interne (l'organisation établit une connexion réseau entre les points d'extrémité qu'elle contrôle de manière à ne pas compter sur des réseaux externes pour protéger la confidentialité ou l'intégrité de l'information transmise dans le

réseau). Les contrôles d'accès à distance s'appliquent aux systèmes autres que les serveurs Web publics ou les systèmes conçus spécifiquement pour un accès public. Le contrôle AC-3 applique les restrictions d'accès associées aux connexions à distance. Contrôles connexes : AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4, PE-17.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour faciliter la surveillance et le contrôle des méthodes d'accès à distance.

Conseils supplémentaires d'amélioration : La surveillance automatisée des sessions d'accès à distance permet aux organisations de vérifier les activités de l'utilisateur sur une variété de composantes de système (p. ex., serveurs, postes de travail, portables) et de s'assurer de la conformité à la politique d'accès à distance.

(2) L'organisation utilise la cryptographie pour protéger la confidentialité et l'intégrité des sessions d'accès à distance. La cryptographie doit être conforme aux exigences du contrôle SC-13.

Conseils supplémentaires d'amélioration : La force de chiffrement du mécanisme est sélectionnée selon les recommandations du document *Guide to Interconnecting Security Domains (ITSG-32) du CSTC* [Référence 23]. Contrôles connexes : SC-8, SC-9, SC-13.

(3) Le système achemine tous les accès à distance par un nombre limité de points de contrôle d'accès gérés.

Conseils supplémentaires d'amélioration : Contrôle connexe : SC-7.

(4) L'organisation autorise l'exécution des commandes privilégiées et l'accès à l'information de sécurité par la méthode d'accès à distance uniquement dans le cas de besoins opérationnels probants et documente le motif de cet accès dans le plan de sécurité du système d'information.

Conseils supplémentaires d'amélioration : Contrôle connexe : AC-6.

(5) L'organisation surveille l'existence de connexions à distance non autorisées au système [*Affectation : fréquence définie par l'organisation*] et prend des mesures appropriées le cas échéant.

(6) L'organisation s'assure que les utilisateurs protègent l'information sur les mécanismes d'accès à distance contre toute utilisation non autorisée et divulgation.

(7) L'organisation s'assure que les sessions d'accès à distance à [*Affectation : liste des fonctions de sécurité et information de sécurité définies par l'organisation*] utilisent [*Affectation : mesures de sécurité supplémentaires définies par l'organisation*] et sont vérifiées.

Conseils supplémentaires d'amélioration : Les mesures de sécurité supplémentaires sont normalement supérieures et plus englobantes que le chiffrement standard en bloc ou de la couche session (p. ex., SSH, RPV avec activation du mode blocage). Contrôles connexes : SC-8, SC-9.

(8) L'organisation désactive [*Affectation : protocoles réseau utilisés dans le système définis par l'organisation et jugés non sécuritaires*] à l'exception des composantes clairement identifiées servant à répondre à des exigences opérationnelles spécifiques.

Conseils supplémentaires d'amélioration : L'organisation peut soit déterminer la sécurité relative du protocole réseau ou baser sa décision sur l'évaluation d'autres entités. Les services Bluetooth et pair à pair sont des exemples de protocoles réseau moins sûrs.

(100) L'accès à distance aux comptes privilégiés est effectué à partir de consoles dédiées à la gestion qui sont gouvernées entièrement par les politiques de sécurité s'appliquant au système. Ceci signifie que, à moins que les politiques de sécurité le permettent, le partage de consoles entre différents systèmes, l'utilisation de techniques de virtualisation sur plateformes supportant des consoles logicielles, et l'accès à l'internet ne sont pas autorisés.

Références :

Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7].
Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].
Guide to Interconnecting Security Domains (ITSG-32) du CSTC [Référence 23].

AC-18 ACCÈS SANS FIL

Contrôle :

(A) L'organisation établit les restrictions d'utilisation et les directives de mise en œuvre de l'accès sans fil.

(B) L'organisation surveille l'existence d'accès sans fil non autorisés au système d'information.

(C) L'organisation autorise l'accès sans fil au système d'information avant la connexion.

(D) L'organisation applique les exigences concernant les connexions sans fil au système d'information.

Conseils supplémentaires : Les technologies sans fil incluent, sans s'y limiter, les micro-ondes, les satellites, les radiocommunications en mode paquet (UHF/VHF), 802.11, et Bluetooth. Les réseaux sans fil utilisent des protocoles d'authentification (p. ex., EAP/TLS, PEAP) qui protègent les justificatifs d'identité et l'authentification mutuelle. Dans certaines situations, les signaux sans fil peuvent se propager au delà des frontières et du contrôle des installations de l'organisation. Contrôles connexes : AC-3, IA-2, IA-3, IA-8, SC-9.

Améliorations du contrôle :

(1) Le système utilise l'authentification et le chiffrement pour se protéger contre l'accès sans fil.

Conseils supplémentaires d'amélioration : L'authentification s'applique aux utilisateurs, aux dispositifs, ou aux deux, le cas échéant. Contrôle connexe : SC-13.

(2) L'organisation surveille la présence de connexions sans fil non autorisées au système d'information, incluant l'analyse des points d'accès sans fil non autorisés [*Affectation : fréquence définie par l'organisation*], et prend des mesures appropriées le cas échéant.

Conseils supplémentaires d'amélioration : Les organisations recherchent proactivement les connexions sans fil non autorisées, incluant l'exécution de balayages rigoureux pour détecter les points d'accès sans fil non autorisés. Le balayage ne se limite pas nécessairement aux installations qui hébergent les systèmes d'information, mais peut être effectué à l'extérieur au besoin pour vérifier que les points d'accès sans fil non autorisés ne sont pas connectés au système.

(3) L'organisation désactive, lorsqu'elle ne prévoit pas les utiliser, les capacités de réseautage sans fil intégrées aux composantes de système avant leur déploiement.

(4) L'organisation ne permet pas aux utilisateurs de configurer eux-mêmes les capacités de réseautage sans fil.

(5) L'organisation restreint les communications sans fil au périmètre qu'elle contrôle.

Conseils supplémentaires d'amélioration : Les mesures que peut prendre l'organisation pour restreindre les communications sans fil au périmètre qu'elle contrôle incluent : (i) la réduction de la puissance d'alimentation de la transmission sans fil pour qu'elle ne puisse traverser le périmètre physique de l'organisation; (ii) l'utilisation de mesures telles TEMPEST pour contrôler les émissions sans fil; et (iii) la configuration de l'accès sans fil pour en faire un accès de type point à point.

Références :

Évaluation des vulnérabilités des assistants numériques personnels (PDA) (ITSPSR-18) du CSTC [Référence 27].
Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21) du CSTC [Référence 28].
Vulnérabilité sur le plan de la sécurité – Ordinateurs portatifs équipés de la technologie WLAN (ITSB-15) du CSTC [Référence 32].
Mesures de sécurité – Appareils électroniques sans fil (ITSB-19) du CSTC [Référence 33].
Sécurité de la messagerie BlackBerry NIP à NIP (ITSB-57) du CSTC [Référence 34].
Conseils sur l'utilisation du protocole TLS (Transport Layer Security) au sein du gouvernement du Canada (ITSB-60) du CSTC [Référence 35].
Critères pour la conception, la fabrication, l'approvisionnement, l'installation et les essais de réception des enceintes blindées contre les radiofréquences (ITSG-02) du CSTC [Référence 36].

AC-19 CONTRÔLE D'ACCÈS AUX DISPOSITIFS MOBILES

Contrôle :

(A) L'organisation établit les restrictions d'utilisation et donne des directives sur les dispositifs mobiles contrôlés par l'organisation.

(B) L'organisation autorise la connexion des dispositifs mobiles qui répondent à ses restrictions d'utilisation et aux directives de mise en œuvre des systèmes d'information organisationnels.

(C) L'organisation surveille les connexions non autorisées des dispositifs mobiles aux systèmes d'information organisationnels.

(D) L'organisation applique les exigences concernant la connexion des dispositifs mobiles à ses systèmes d'information.

(E) L'organisation désactive les fonctions du système d'information qui permettent l'exécution automatique du code des dispositifs mobiles sans l'autorisation de l'utilisateur.

(F) L'organisation remet, en conformité avec ses politiques et procédures, des dispositifs mobiles spécialement configurés aux individus qui se déplacent dans des emplacements qui, selon elle, présentent des risques importants.

(G) L'organisation applique [*Affectation : mesures d'inspection et préventives définies par l'organisation*], en conformité avec ses politiques et procédures, aux dispositifs mobiles à leur retour des emplacements qui, selon elle, présentent des risques importants.

Conseils supplémentaires : Les dispositifs mobiles incluent les supports de stockage portables (p. ex., clé USB, lecteurs de disques rigides externes) et les dispositifs portables de traitement et de communications dotés d'une capacité de stockage d'information (p. ex., portables, assistants numériques, téléphones cellulaires, caméras numériques, et matériel d'enregistrement sonore). Les dispositifs mobiles contrôlés par l'organisation incluent les dispositifs pour lesquels l'organisation est autorisée à préciser et appliquer des exigences spécifiques en matière de contrôle de sécurité. Les restrictions d'utilisation et les directives de mise en œuvre des dispositifs mobiles incluent, par exemple, la gestion de la configuration, l'identification et l'authentification, la mise en œuvre des logiciels de protection obligatoires (p. ex., détecteur de code malveillant, pare-feu), l'analyse aux fins de détection de code malveillant, la mise à jour du logiciel antivirus, la recherche des mises à jour et des rustines critiques, l'exécution des contrôles d'intégrité du système d'exploitation principal (et autre logiciel résident, le cas échéant), et la désactivation de tout matériel inutile (p. ex., sans fil, infrarouge). Les exemples de fonctions système capables d'exécuter automatiquement le code incluent AutoRun et AutoPlay.

Les politiques et procédures de l'organisation concernant les dispositifs mobiles utilisés par des employés qui partent en voyage ou en reviennent incluent, par exemple : déterminer les emplacements à risque qui seront visités, définir les configurations requises pour les dispositifs, veiller à ce que les dispositifs soient configurés tel que prévu avant le début du voyage et appliquer des mesures spécifiques aux dispositifs au retour. Les dispositifs mobiles spécialement configurés incluent, par exemple, les ordinateurs dotés de disques rigides nettoyés et d'un nombre limité d'applications et qui ont fait l'objet d'un renforcement supplémentaire (p. ex., paramètres de configuration plus stricts). Les mesures particulières appliquées aux dispositifs à leur retour incluent, par exemple, un examen aux fins de détection d'indices de trafiquage physique et le nettoyage et la recréation d'image du lecteur de disque rigide. La protection de l'information contenue dans les dispositifs mobiles est abordée dans la famille des contrôles concernant la protection des supports. Contrôles connexes : MP-4, MP-5.

Améliorations du contrôle :

(1) L'organisation restreint l'utilisation des supports amovibles inscriptibles dans ses systèmes d'information.

(2) L'organisation interdit l'utilisation des supports amovibles personnels dans ses systèmes d'information.

(3) L'organisation interdit l'utilisation de supports amovibles dont le propriétaire est inconnu dans ses systèmes d'information.

Conseils supplémentaires d'amélioration : Les supports amovibles dont le propriétaire est identifiable (p. ex., individu, organisation ou projet) aident à réduire le risque d'utilisation de cette technologie; on sait ainsi à qui attribuer la responsabilité de régler les vulnérabilités connues des supports concernés (p. ex., insertion de code malveillant).

(4) L'organisation :

(a) Interdit l'utilisation de dispositifs mobiles non classifiés dans les installations qui hébergent des systèmes qui traitent, stockent ou transmettent de l'information classifiée, sauf si l'agent d'autorisation concerné le permet; et

(b) Applique les restrictions qui suivent aux individus autorisés à utiliser des dispositifs mobiles dans les installations qui hébergent des systèmes qui traitent, stockent ou transmettent de l'information classifiée :

- Il est interdit de connecter des dispositifs mobiles non classifiés à des systèmes qui traitent de l'information classifiée;
- La connexion de dispositifs mobiles non classifiés à des systèmes qui traitent de l'information non classifiée requiert l'approbation de l'agent d'autorisation concerné;
- Il est interdit d'utiliser des modems internes ou externes ou des interfaces sans fil avec les dispositifs mobiles (i.e. ils doivent être désactivés); et
- Les dispositifs mobiles et l'information qu'ils contiennent peuvent faire l'objet d'examens et (ou) d'inspections ponctuels par [*Affectation : agents de sécurité définis par l'organisation*]; si l'inspection confirme la présence d'information classifiée, la politique de traitement des incidents est appliquée.

(100) L'organisation s'assure que les utilisateurs désactivent les dispositifs sans fil dotés d'une capacité de transmission de la voix, ou qu'ils en retirent manuellement le microphone lorsqu'ils participent à des réunions au cours desquelles il y a partage d'information classifiée, protégée B ou protégée C, conformément à la *Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT* [Référence 8].

Références :

Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].
Évaluation des vulnérabilités des assistants numériques personnels (PDA) (ITSPSR-18) du CSTC [Référence 27].
Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21) du CSTC [Référence 28].
Vulnérabilité sur le plan de la sécurité – Ordinateurs portatifs équipés de la technologie WLAN (ITSB-15) du CSTC [Référence 32].
Mesures de sécurité – Appareils électroniques sans fil (ITSB-19) du CSTC [Référence 33].
Sécurité de la messagerie BlackBerry NIP à NIP (ITSB-57) du CSTC [Référence 34].

AC-20 UTILISATION DES SYSTÈMES D'INFORMATION EXTERNES

Contrôle :

(A) L'organisation, conformément aux relations de confiance établies avec d'autres organisations qui possèdent, exploitent et (ou) maintiennent des systèmes d'information externes, définit les modalités selon lesquelles des individus, à partir de systèmes externes, sont autorisés à accéder au système d'information.

(B) L'organisation, conformément aux relations de confiance établies avec d'autres organisations qui possèdent, exploitent et (ou) maintiennent des systèmes d'information externes, définit les modalités selon lesquelles des individus, à partir de systèmes externes, sont autorisés à traiter, stocker et (ou) transmettre de l'information qu'elle contrôle.

Conseils supplémentaires : Les systèmes d'information externes sont des systèmes ou des composantes de système non soumis à la limite d'autorisation établie par l'organisation et sur lesquels elle n'exerce normalement aucune supervision ni autorité directes au plan de l'application des contrôles de sécurité ou de l'évaluation de l'efficacité de ces contrôles. Ils incluent, sans s'y limiter (i) les systèmes d'information personnels (p. ex., ordinateurs, téléphones cellulaires ou assistants numériques), (ii) les dispositifs de traitement et de

communications privés hébergés dans des installations commerciales ou publiques (p. ex., hôtels, centres de congrès ou aéroports), (iii) les systèmes d'information appartenant à des organisations non gouvernementales ou dont le contrôle relève de ces organisations et (iv) les systèmes d'information du GC qui ne sont ni la propriété de l'organisation, ni exploités ou contrôlés sous sa supervision directe et son autorité. Dans le cas de certains systèmes externes, plus particulièrement ceux exploités par d'autres organisations du GC, incluant les organisations qui leur sont subordonnées, les relations de confiance établies entre ces organisations et l'organisation concernée peuvent être telles qu'aucune modalité explicite n'est requise. Dans les faits, les systèmes de ces organisations ne sont pas considérés des systèmes externes. Ces situations se produisent normalement, par exemple, lorsqu'un partage existait déjà ou qu'une entente de confiance (implicite ou explicite) avait été établie entre les organisations subordonnées de ces organisations du GC, ou lorsque de telles ententes sont stipulées dans les lois du GC et les politiques, directives et normes concernées du SCT. Les individus autorisés incluent les employés de l'organisation, les entrepreneurs ou toute autre personne autorisée à accéder au système de l'organisation et à laquelle l'organisation est en droit d'imposer des règles de conduite en matière d'accès aux systèmes. Il n'est pas nécessaire que les restrictions qu'une organisation impose aux individus autorisés soient uniformes puisqu'elles peuvent varier selon les relations de confiance entre les organisations. Ainsi, une organisation peut imposer des restrictions de sécurité plus strictes à un entrepreneur qu'à un gouvernement provincial ou municipal, ou au gouvernement fédéral.

Ce contrôle ne concerne pas l'utilisation de systèmes externes pour accéder à des interfaces publiques permettant d'utiliser les systèmes et l'information de l'organisation. L'organisation établit les modalités d'utilisation des systèmes externes en conformité avec ses politiques et procédures en matière de sécurité. Les modalités définissent au minimum (i) les types d'applications accessibles de l'extérieur et (ii) les niveaux maximum de sécurité de l'information qui peut être traitée, stockée et transmise dans le système externe. Ce contrôle définit les autorisations d'accès appliquées par le contrôle AC-3, les exigences relatives aux règles de conduite appliquées par le contrôle PL-4 et les règles d'établissement de session appliquées par le contrôle AC-17. Contrôles connexes : AC-3, AC-17, PL-4.

Améliorations du contrôle :

(1) L'organisation permet à des individus autorisés d'utiliser un système externe pour accéder à son système d'information ou pour traiter, stocker ou transmettre de l'information sous son contrôle seulement lorsqu'elle :

(a) Peut s'assurer que le système externe applique les contrôles de sécurité requis tel que stipulé dans sa politique de sécurité de l'information et le plan de sécurité; ou

(b) A approuvé les ententes de connexion ou de traitement avec l'entité organisationnelle qui héberge le système externe.

(2) L'organisation limite, dans les systèmes externes, l'utilisation par des individus autorisés des supports de stockage amovibles qu'elle contrôle.

Conseils supplémentaires d'amélioration : Les limites d'utilisation, dans les systèmes externes, des supports de stockage amovibles contrôlés par l'organisation par des individus autorisés peuvent inclure, par exemple, l'interdiction absolue d'utiliser ces dispositifs ou des restrictions et des modalités sur la façon de les utiliser.

Références :

Aucune.

AC-21 COLLABORATION ET PARTAGE D'INFORMATION ENTRE UTILISATEURS

Contrôle :

(A) L'organisation facilite le partage d'information en permettant aux utilisateurs autorisés de déterminer si les autorisations d'accès accordées aux partenaires de partage respectent les restrictions d'accès à l'information

en tenant compte [*Affectation : circonstances de partage d'information définies par l'organisation où l'utilisateur doit faire preuve de discrétion*].

(B) L'organisation utilise [*Affectation : liste définie par l'organisation des circonstances de partage d'information et des mécanismes automatisés ou des processus manuels requis*] pour aider les utilisateurs à prendre des décisions concernant le partage d'information et la collaboration.

Conseils supplémentaires : Le contrôle s'applique à l'information susceptible de faire l'objet de restrictions (p. ex., information privilégié de nature médicale, contractuelle, propriétaire et personnelle, programmes d'accès spéciaux) basées sur un mode quelconque de détermination formelle ou administrative. Selon la circonstance de partage d'information, le partenaire de partage peut être un individu, un groupe ou une organisation et l'information peut être définie en fonction d'un contenu, d'un type ou d'une catégorie de sécurité spécifiques. Contrôle connexe : AC-3.

Améliorations du contrôle :

(1) Le système utilise des mécanismes automatisés pour permettre aux utilisateurs autorisés de prendre des décisions concernant le partage d'information en tenant compte des autorisations d'accès des partenaires de partage et des restrictions d'accès à l'information à partager

(100) L'organisation, suite à des ententes écrites, veille à prendre les mesures de protection appropriées de l'information sensible partagée avec d'autres gouvernements et organisations.

Références :

Norme Sécurité relative à l'organisation et l'administration du CST [Référence 14].

AC-22 CONTENU ACCESSIBLE AU PUBLIC

Contrôle :

(A) L'organisation désigne les individus autorisés à afficher de l'information dans les systèmes organisationnels accessibles au public.

(B) L'organisation forme les individus autorisés afin de s'assurer que l'information accessible au public ne contienne aucune information sensible confidentielle.

(C) L'organisation examine le contenu proposé de l'information mise à la disposition du public pour s'assurer qu'elle ne contienne aucune information sensible confidentielle avant qu'elle ne soit affichée dans le système organisationnel.

(D) L'organisation examine [*Affectation : fréquence définie par l'organisation*] le contenu de l'information mise à la disposition du public pour s'assurer qu'elle ne contient aucune information sensible confidentielle.

(E) L'organisation, le cas échéant, retire toute information sensible confidentielle du système organisationnel accessible au public.

Conseils supplémentaires : L'information sensible confidentielle est toute information à laquelle le public général n'est pas autorisé à accéder, conformément aux lois du GC et aux politiques, directives et normes concernées du SCT. L'information protégée en vertu de la Loi sur la protection des renseignements personnels et les renseignements propriétaires des fournisseurs sont des exemples de ce type d'information. Ce contrôle concerne l'affichage d'information dans un système organisationnel accessible au public sans l'application des mesures d'identification ou d'authentification habituelles. L'affichage d'information dans les systèmes non organisationnels fait l'objet d'une politique distincte de l'organisation. Contrôles connexes : AC-3, AU-13.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

4.2 FAMILLE : SENSIBILISATION ET FORMATION

CLASSE : OPÉRATIONNELLE

AT-1 POLITIQUE ET PROCÉDURES DE FORMATION ET DE SENSIBILISATION À LA SÉCURITÉ

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique de formation et de sensibilisation à la sécurité formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de formation et de sensibilisation à la sécurité et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de sensibilisation et de formation à la sécurité. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique de formation et de sensibilisation à la sécurité peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures de formation et de sensibilisation à la sécurité peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique de formation et de sensibilisation à la sécurité. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].

AT-2 SENSIBILISATION À LA SÉCURITÉ

Contrôle :

(A) L'organisation dispense une formation de base de sensibilisation à la sécurité à tous les utilisateurs du système d'information (incluant les gestionnaires, les cadres supérieurs et les entrepreneurs) dans le cadre de la formation initiale des nouveaux utilisateurs; la formation est offerte lorsque les changements apportés au système le justifient, et à tous les [*Affectation : fréquence définie par l'organisation*] par la suite.

Conseils supplémentaires : L'organisation détermine le contenu des cours de formation et des techniques de sensibilisation à la sécurité en tenant compte des exigences de l'organisation et des systèmes d'information auxquels le personnel est autorisé à accéder. Le contenu inclut une connaissance de base du besoin de sécuriser l'information et des mesures que doivent prendre les utilisateurs pour maintenir la sécurité et intervenir en cas d'incidents de sécurité suspects. Il inclut également une sensibilisation au besoin de protéger les opérations conformément au programme de sécurité de l'information de l'organisation. Les techniques de sensibilisation

peuvent inclure, par exemple, l'apposition d'affiches, la distribution de fournitures de bureau étiquetées de rappels, l'envoi de courriels d'avis et (ou) de notification par les cadres supérieurs de l'organisation, l'affichage de messages lors des connexions et la tenue d'événements de sensibilisation.

Améliorations du contrôle :

(1) L'organisation inclut dans la formation des exercices pratiques de sensibilisation qui simulent des cyberattaques réelles.

Conseils supplémentaires d'amélioration : Les exercices pratiques peuvent inclure, par exemple, des tentatives sans préavis de collecte d'information par des mécanismes d'ingénierie sociale, l'obtention d'un accès non autorisé ou la simulation de l'incidence négative liée à l'ouverture de pièces jointes malveillantes ou à l'utilisation de liens vers des sites Web malveillants.

Références :

Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].

AT-3 FORMATION À LA SÉCURITÉ

Contrôle :

(A) L'organisation offre une formation à la sécurité axée sur les rôles (i) avant d'autoriser l'accès au système ou l'exécution des tâches reliées au poste de l'utilisateur, (ii) lorsque les modifications apportées au système l'exigent et (iii) [*Affectation : fréquence définie par l'organisation*] par la suite.

Conseils supplémentaires : L'organisation détermine le contenu de la formation à la sécurité en tenant compte des rôles et responsabilités assignés, des exigences spécifiques de l'organisation et des systèmes auxquels le personnel est autorisé à accéder. En plus, elle offre, pour leur permettre de s'acquitter de leurs tâches, une formation technique en sécurité aux gestionnaires de système d'information, aux administrateurs de système et de réseau, au personnel chargé des activités indépendantes de vérification et de validation, aux évaluateurs des contrôles de sécurité et aux autres employés qui ont accès au logiciel de système. La formation à la sécurité s'intéresse aux rôles et responsabilités techniques, opérationnels et de gestion associés aux contrôles de sécurité physiques, techniques et du personnel. L'organisation dispense également la formation nécessaire aux individus pour leur permettre de s'acquitter de leurs responsabilités en matière de sécurité des opérations tel que stipulé dans son programme de sécurité de l'information. Contrôles connexes : AT-2, SA-3.

Améliorations du contrôle :

(1) L'organisation assure la formation initiale et [*Affectation : fréquence définie par l'organisation*] des employés sur l'utilisation et l'application des contrôles environnementaux.

Conseils supplémentaires d'amélioration : Les contrôles environnementaux incluent, par exemple, les dispositifs et (ou) systèmes de suppression et de détection des incendies, les systèmes de gicleurs, les extincteurs manuels, les boyaux d'arrosage fixes, les détecteurs de fumée, les dispositifs de contrôle de la température et de l'humidité, la CVC et alimentation de l'installation.

(2) L'organisation assure la formation initiale et [*Affectation : fréquence définie par l'organisation*] des employés sur l'utilisation et l'application des contrôles de sécurité physique.

Conseils supplémentaires d'amélioration : Les contrôles de sécurité physique incluent, par exemple, les dispositifs de contrôle d'accès physique, les avertisseurs d'intrusion physique, l'équipement de contrôle et de surveillance et les agents de sécurité (procédures de déploiement et d'exploitation).

Références :

Aucune.

AT-4 DOSSIERS DE FORMATION À LA SÉCURITÉ

Contrôle :

(A) L'organisation documente et surveille les activités individuelles de formation à la sécurité des systèmes d'information, incluant la formation de sensibilisation de base et la formation spécifique à la sécurité des systèmes d'information.

(B) L'organisation conserve les dossiers de formation individuels pendant [*Affectation : durée définie par l'organisation*].

Conseils supplémentaires : Une organisation peut juger nécessaire d'offrir des programmes de formation et de développer des plans de formation individuels; toutefois, ce contrôle n'inclut aucune obligation à l'égard ni de l'un ni de l'autre. À la discrétion de l'organisation, chaque superviseur peut documenter ses propres cours de formation spécialisée.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

AT-5 CONTACTS AVEC LES GROUPES ET ASSOCIATIONS DE SÉCURITÉ

Contrôle :

(A) L'organisation établit et institutionnalise les contacts avec certains groupes et associations de la collectivité de la sécurité afin de faciliter l'éducation et la formation permanentes de son personnel.

(B) L'organisation établit et institutionnalise les contacts avec certains groupes et associations de la collectivité de la sécurité pour se tenir au fait des plus récentes pratiques, techniques et technologies recommandées en matière de sécurité.

(C) L'organisation établit et institutionnalise les contacts avec certains groupes et associations de la collectivité de la sécurité pour partager des renseignements actuels sur la sécurité, incluant les menaces, les vulnérabilités et les incidents.

Conseils supplémentaires : Le maintien de contacts permanents avec certains groupes et associations de sécurité est de la plus haute importance dans un environnement où la technologie et les menaces évoluent rapidement et de manière dynamique. Les groupes et associations de sécurité peuvent inclure, par exemple, les groupes d'intérêts spéciaux, les forums spécialisés, les associations professionnelles, les groupes de nouvelles et (ou) les groupes de pairs professionnels d'organisations similaires. Les groupes et associations choisis sont conformes aux exigences de la mission et (ou) opérationnels de l'organisation. Les activités de partage d'information sur les menaces, les vulnérabilités et les incidents reliés aux systèmes d'information sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

4.3 FAMILLE : VÉRIFICATION ET RESPONSABILITÉ

CLASSE : TECHNIQUE

AU-1 POLITIQUE ET PROCÉDURES DE VÉRIFICATION ET DE RESPONSABILISATION

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique de vérification et de responsabilisation formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de vérification et de responsabilisation et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de vérification et de responsabilisation. La politique et les procédures de vérification et de responsabilisation sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique de vérification et de responsabilisation peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures de vérification et de responsabilisation peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique de vérification et de responsabilisation. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].
Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].

AU-2 Événements vérifiables

Contrôle :

(A) L'organisation détermine, à partir d'une évaluation des risques et des besoins opérationnels et de la mission, la capacité du système d'information de vérifier les événements suivants : [*Affectation : liste des événements vérifiables définie par l'organisation*].

(B) L'organisation coordonne la fonction de vérification de la sécurité avec d'autres entités organisationnelles ayant les même besoins pour favoriser le soutien mutuel et faciliter la sélection des événements vérifiables.

(C) L'organisation explique pourquoi la liste des événements vérifiables est jugée adéquate pour soutenir les enquêtes après le fait des incidents de sécurité.

(D) L'organisation détermine, à partir de l'information actuelle sur les menaces et de l'évaluation continue des risques, si les événements suivants doivent être vérifiés dans le système d'information : [*Affectation : sous-ensemble défini par l'organisation des événements vérifiables définis en AU-2 a. qui doivent être vérifiés, incluant la fréquence de vérification (ou la situation qui justifie la vérification) de chacun*].

Conseils supplémentaires : Le but de ce contrôle est de permettre à l'organisation d'indiquer que les événements qui doivent être vérifiés sont importants et pertinents pour la sécurité du système. Pour établir un équilibre entre les besoins de vérification et les autres besoins du système d'information, ce contrôle exige également que soit déterminé le sous-ensemble d'événements vérifiables qui seront vérifiés à un moment précis. Par exemple, l'organisation peut déterminer que le système doit être en mesure de journaliser tous les accès de fichier, réussis ou non, tout en recourant à cette capacité uniquement dans des circonstances particulières en raison du lourd impact qu'elle a sur le rendement du système. En outre, les dossiers de vérification peuvent être créés à différents niveaux d'abstraction, incluant le niveau paquet, puisque l'information parcoure tout le réseau. La sélection de bon niveau d'abstraction est critique pour la capacité de vérification et peut faciliter l'identification des causes profondes des problèmes. Contrôle connexe : AU-3.

Améliorations du contrôle :

(1) [Annulée : Intégrée au contrôle AU-12].

(2) [Annulée : Intégrée au contrôle AU-12].

(3) L'organisation examine et met à jour la liste des événements vérifiables [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires d'amélioration : La liste des événements vérifiables est définie dans le contrôle AU-2.

(4) L'organisation inclut l'exécution de fonctions privilégiées dans la liste des événements à vérifier par le système.

Références :

Aucune.

AU-3 CONTENU DES DOSSIERS DE VÉRIFICATION

Contrôle :

(A) Le système d'information produit des dossiers de vérification qui contiennent suffisamment d'information pour permettre, au minimum, d'établir le type d'événement qui s'est produit, la date et l'heure de l'événement, l'endroit où il s'est produit, sa source, son résultat (réussite ou échec) et l'identité de tous les utilisateurs ou sujets qui lui sont associés.

Conseils supplémentaires : Le contenu du dossier de vérification jugé nécessaire pour satisfaire aux exigences de ce contrôle inclut, par exemple, les timbres horodateurs, les adresses source et de destination, les identificateurs d'utilisateur et (ou) de processus, des descriptions de l'événement, une indication de la réussite ou de l'échec, les noms des fichiers concernés et les règles de contrôle d'accès ou de flux invoquées. Contrôles connexes : AU-2, AU-8.

Améliorations du contrôle :

(1) Le système inclut [*Affectation : information supplémentaire et plus détaillée définie par l'organisation*], répartie par type, emplacement ou sujet, dans les dossiers de vérification des événements.

Conseils supplémentaires d'amélioration : L'enregistrement plein texte des commandes privilégiées ou les identités individuelles des utilisateurs d'un compte de groupe sont des exemples d'information détaillée dont l'organisation peut avoir besoin dans les dossiers de vérification.

(2) L'organisation centralise la gestion du contenu des dossiers de vérification produits par [*Affectation : composantes de système définies par l'organisation*].

Références :

Aucune.

AU-4 CAPACITÉ DE STOCKAGE DES VÉRIFICATIONS

Contrôle :

(A) L'organisation attribue la capacité de stockage des dossiers de vérification et configure les vérifications de manière à réduire la probabilité de dépassement de cette capacité.

Conseils supplémentaires : L'organisation tient compte des types de vérification à effectuer et des exigences de traitement pour attribuer la capacité de stockage. Contrôles connexes : AU-2, AU-5, AU-6, AU-7, SI-4.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

AU-5 INTERVENTION EN CAS DE PROBLÈMES DE TRAITEMENT

Contrôle :

(A) Le système d'information avertit les agents désignés de l'organisation dans l'éventualité d'un problème de traitement des vérifications.

(B) Le système d'information prend les mesures supplémentaires suivantes : [*Affectation : mesures à prendre définies par l'organisation (p. ex., arrêt du système, écrasement des vieux fichiers de vérification, arrêt de production de fichiers de vérification)*].

Conseils supplémentaires : Les problèmes de traitement des vérifications incluent, par exemple, les erreurs de logiciel et (ou) de matériel, les défaillances des mécanismes de saisie des vérifications et l'atteinte ou le dépassement de la capacité de stockage des vérifications. Contrôle connexe : AU-4.

Améliorations du contrôle :

(1) Le système produit un avertissement lorsque le volume attribué de stockage des dossiers de vérification atteint [*Affectation : pourcentage défini par l'organisation*] de la capacité maximale.

(2) Le système produit un avertissement en temps réel lorsque les événements suivants liés à la défaillance d'une vérification se produisent : [*Affectation : événements définis par l'organisation liés à la défaillance d'une vérification qui nécessitent un avertissement en temps réel*].

(3) Le système applique des seuils de volume de trafic configurables représentant la capacité de vérification du trafic réseau et [*Sélection : rejette ou retarde*] le trafic au delà de ces seuils.

(4) Le système s'arrête obligatoirement dans l'éventualité d'une défaillance de la vérification, sauf lorsqu'il existe une capacité de vérification de secours.

Références :

Aucune.

AU-6 EXAMEN, ANALYSE ET RAPPORTS DE Vérification

Contrôle :

(A) L'organisation examine et analyse les dossiers de vérification du système d'information [*Affectation : fréquence définie par l'organisation*] pour déceler toute activité inappropriée ou inhabituelle et remet ses constatations à ses agents désignés.

(B) L'organisation ajuste le niveau d'examen, d'analyse et de rapports de vérification du système d'information lorsqu'il y a une variation du risque pour les activités et les biens organisationnels, les individus, les autres organisations ou le Canada suite à la réception de renseignements et d'information concernant le respect des lois, ou d'information en provenance d'autres sources crédibles.

Conseils supplémentaires : Contrôles connexes : AU-7, AC-5.

Améliorations du contrôle :

(1) Le système intègre les processus d'examen, d'analyse et de rapports des vérifications pour soutenir les processus organisationnels d'enquête et d'intervention en cas d'activités suspectes.

(2) [Annulée : Intégrée au contrôle SI-4].

(3) L'organisation analyse et met en corrélation les dossiers de vérification des différents dépôts afin de se sensibiliser à sa situation globale.

(4) Le système centralise l'examen et l'analyse des dossiers de vérification de plusieurs composantes du système.

Conseils supplémentaires d'amélioration : Le produit SIM (Security Information Management) est un exemple de mécanisme automatisé d'examen et d'analyse centralisés. Contrôle connexe : AU-2.

(5) L'organisation intègre l'analyse des dossiers de vérification à l'information d'analyse des vulnérabilités, aux données de rendement et à l'information sur la surveillance de réseau pour accroître sa capacité d'identification des activités inappropriées ou inhabituelles.

Conseils supplémentaires d'amélioration : Un outil de gestion des événements de sécurité et des systèmes d'information peut faciliter le regroupement et la consolidation des dossiers de vérification produits par les nombreuses composantes de système ainsi que l'analyse et la mise en corrélation des dossiers de vérification. L'utilisation des scripts normalisés d'analyse des dossiers de vérification développés par l'organisation (incluant des ajustements locaux, au besoin) offre une approche plus rentable de l'analyse de l'information collectée dans les dossiers de vérification. La corrélation de l'information contenue dans les dossiers de vérification avec celle produite par l'analyse des vulnérabilités est importante et permet d'établir la justesse des analyses de vulnérabilités et de la corrélation entre les événements de détection des attaques et les résultats des analyses. Contrôles connexes : AU-7, RA-5, SI-4.

(6) L'organisation met en corrélation l'information des dossiers de vérification avec celle obtenue lors de la surveillance de l'accès physique pour accroître la capacité d'identification des activités suspectes, inappropriées, inhabituelles ou malveillantes.

Conseils supplémentaires d'amélioration : Contrôle connexe : PE-6.

(7) L'organisation précise, dans la politique de vérification et de responsabilisation, les mesures autorisées pour chaque processus de système, rôle et (ou) utilisateur approuvés.

Conseils supplémentaires d'amélioration : Les mesures autorisées pour chaque processus de système, rôle et (ou) utilisateur associés à l'examen, à l'analyse et aux rapports des dossiers de vérification incluent, par exemple, la lecture, l'écriture, l'annexion et la suppression.

(8) [Annulée : Intégrée au contrôle SI-4].

(9) L'organisation effectue, dans un système d'information physique spécialisé, une analyse plein texte des fonctions privilégiées exécutées.

Références :

Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8], *Norme opérationnelle de sécurité - Programme de planification de la continuité des activités (PCA) du SCT* [Référence 12].

AU-7 RÉDUCTION DES VÉRIFICATIONS ET PRODUCTIONS DES RAPPORTS

Contrôle :

(A) Le système d'information offre une capacité de réduction des vérifications et de production des rapports.

Conseils supplémentaires : La capacité de réduction des vérifications et de production des rapports permet de satisfaire quasi en temps réel aux exigences d'examen, d'analyse et de rapports de vérification décrites au contrôle AU-6 et de soutenir les enquêtes après le fait sur les incidents de sécurité. Les outils de réduction des vérifications et de production de rapports ne modifient en rien les dossiers de vérification originaux. Contrôle connexe : AU-6.

Améliorations du contrôle :

(1) Le système permet, à partir de critères d'événement sélectionnables, de traiter automatiquement les dossiers de vérification des événements d'intérêt.

Références :

Aucune.

AU-8 TIMBRES HORODATEURS

Contrôle :

(A) Le système d'information utilise des horloges de système internes pour produire des timbres horodateurs pour les dossiers de vérification.

Conseils supplémentaires : Les timbres horodateurs produits par le système incluent la date et l'heure. L'heure peut être exprimée sous forme de TUC, prolongement moderne du TMG, ou d'heure locale avec extension TUC. Contrôle connexe : AU-3.

Améliorations du contrôle :

(1) Le système synchronise les horloges internes [*Affectation : fréquence définie par l'organisation*] en utilisant [*Affectation : source horaire autorisée définie par l'organisation*].

Références :

Aucune.

AU-9 PROTECTION DE L'INFORMATION DE VÉRIFICATION

Contrôle :

(A) Le système d'information protège l'information de vérification et les outils de vérification contre tout accès, modification et suppression non autorisés.

Conseils supplémentaires : L'information de vérification inclut toute information (p. ex., dossiers de vérification, paramètres de vérification et rapports de vérification) nécessaire à la réussite de l'activité de vérification de l'information. Contrôles connexes : AC-3, AC-6.

Améliorations du contrôle :

(1) Le système produit les dossiers de vérification sur des supports matériels non réinscriptibles.

(2) Le système effectue une sauvegarde des dossiers de vérification [*Affectation : fréquence définie par l'organisation*] dans un système ou des supports différents du système qui fait l'objet de la vérification.

(3) Le système utilise des mécanismes cryptographiques pour protéger l'intégrité de l'information et des outils de vérification.

Conseils supplémentaires d'amélioration : Les exemples de mécanismes cryptographiques de protection de l'intégrité incluent le calcul et l'application d'un hachage cryptographique asymétrique, la protection de la confidentialité de la clé utilisée pour produire le hachage, et l'utilisation de la clé publique pour vérifier l'information de hachage.

(4) L'organisation :

(a) Accorde l'accès à la fonction de gestion de la vérification uniquement à un nombre restreint d'utilisateurs privilégiés; et

(b) Protège les dossiers de vérification des accès distants aux comptes privilégiés et des exécutions de fonctions privilégiées.

Conseils supplémentaires d'amélioration : La vérification peut ne pas être fiable lorsqu'elle est effectuée par le système d'information auquel l'utilisateur vérifié a un accès privilégié. L'utilisateur privilégié peut nuire à la vérification ou en modifier les dossiers. L'amélioration de contrôle aide à atténuer ce risque en exigeant d'établir une distinction entre l'accès privilégié lié à la fonction de vérification et celui lié aux autres fonctions; ainsi, on réduit le nombre d'utilisateurs possédant des privilèges liés à la vérification. On peut également réduire ce risque en effectuant, par exemple, les activités de vérification sur un système d'information distinct ou en utilisant des supports de stockage qui ne peuvent être modifiés (p. ex., dispositifs non réinscriptibles).

Références :

Aucune.

AU-10 NON-RÉPUDIATION

Contrôle :

(A) Le système d'information offre une protection contre quiconque nie faussement avoir effectué une opération particulière.

Conseils supplémentaires : Les exemples d'opérations particulières effectuées par des individus incluent la création d'information, l'envoi de message, l'approbation d'information (p. ex., confirmation d'un accord ou signature d'un contrat) et la réception de message. La non-répudiation protège les individus contre toute déclaration ultérieure d'un auteur qui nie être le créateur d'un document particulier, d'un émetteur qui nie avoir transmis un message, d'un destinataire qui nie avoir reçu un message ou d'un signataire qui nie avoir signé un document. Les services de non-répudiation peuvent servir à déterminer si l'information provient d'un individu particulier, si une personne à pris des mesures particulières (p. ex., envoi d'un courriel, signature d'un contrat, approbation d'une demande d'approvisionnement) ou si elle a reçu certains renseignements. Plusieurs techniques ou mécanismes permettent d'obtenir ces services (p. ex., signatures numériques, reçus numériques de message).

Améliorations du contrôle :

(1) Le système associe l'identité du producteur d'information à l'information.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle satisfait aux exigences de vérification selon lesquelles les agents concernés de l'organisation doivent pouvoir être en mesure d'identifier l'auteur d'une information particulière dans l'éventualité d'un transfert d'information. La nature et la force du lien entre l'auteur et l'information concernée sont déterminées et approuvées par les agents appropriés de l'organisation en fonction des catégories de sécurité de l'information et des facteurs de risque correspondants.

(2) Le système valide le lien entre l'identité du producteur de l'information et l'information.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle vise à atténuer le risque que l'information soit modifiée entre sa production et son examen. La validation des liens peut être effectuée, par exemple, par l'utilisation de totaux de contrôle cryptographiques.

(3) Le système conserve, dans une chaîne de possession préétablie, l'identité et les justificatifs d'identité de l'examinateur et (ou) de l'émetteur de tous les renseignements examinés ou diffusés.

Conseils supplémentaires d'amélioration : Si l'examinateur est une personne ou si la fonction d'examen est automatisée mais distincte de la fonction de diffusion et (ou) de transfert, le système d'information associe à l'information, et à l'étiquette de l'information, l'identité de l'examinateur de l'information à diffuser. Dans le cas d'un examen effectué par une personne, l'amélioration de contrôle fournit aux agents concernés de l'organisation le moyen d'identifier l'examinateur et le diffuseur de l'information. Dans le cas d'un examen automatisé, elle permet de s'assurer que seules des fonctions d'examen approuvées ont été utilisées.

(4) Le système valide le lien entre l'identité de l'examinateur et l'information au point de transfert et (ou) de diffusion de l'information, avant que les renseignements ne soient transférés et (ou) diffusés d'un domaine de sécurité à un autre.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle vise à atténuer le risque que l'information soit modifiée entre son examen et son transfert et (ou) sa diffusion.

(5) L'organisation utilise un mécanisme cryptographique conforme aux exigences du contrôle SC-13 concernant l'application des signatures numériques.

Conseils supplémentaires d'amélioration : Contrôle connexe : SC-13.

Références :

Guide sur l'authentification des utilisateurs pour les systèmes TI (ITSG-31) du CSTC [Référence 19].

AU-11 CONSERVATION DES DOSSIERS DE VÉRIFICATION

Contrôle :

(A) L'organisation conserve les dossiers de vérification pendant [*Affectation : durée définie par l'organisation et conforme à la politique de conservation des dossiers*] pour soutenir les enquêtes après le fait effectuées sur les incidents de sécurité et satisfaire aux exigences règlementaires et organisationnelles de conservation de l'information.

Conseils supplémentaires : L'organisation conserve les dossiers de vérification jusqu'à ce qu'il soit établi qu'ils ne sont plus requis aux fins administratives, juridiques, opérationnelles ou autres. Cette responsabilité inclut, par exemple, la conservation et la disponibilité des dossiers de vérification pour répondre aux demandes de nature juridique, aux assignations à témoigner et aux mesures d'application des lois. L'organisation développe et diffuse des catégories standard de dossier de vérification en fonction de ces types de mesures ainsi que des processus d'intervention standard pour chaque type.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

AU-12 PRODUCTION DES DOSSIERS DE VÉRIFICATION

Contrôle :

(A) Le système d'information inclut une capacité de production de dossiers de vérification pour les événements vérifiables définis dans la liste de [*Affectation : composantes de système définies par l'organisation*] du contrôle AU-2.

(B) Le système d'information permet au personnel désigné de l'organisation de sélectionner, par composante de système particulière, les événements vérifiables qui doivent être vérifiés.

(C) Le système d'information produit des dossiers de vérification pour les événements vérifiables définis dans la liste du contrôle AU-2 et dont le contenu est défini au contrôle AU-3.

Conseils supplémentaires : Des dossiers de vérification peuvent être produits par différentes composantes du système d'information. La liste des événements vérifiables inclut les événements qui doivent être vérifiés. Cet ensemble d'événements est normalement un sous-ensemble de la liste de tous les événements pour lesquels le système peut produire des dossiers de vérification (c.-à-d., événements vérifiables). Contrôles connexes : AU-2, AU-3.

Améliorations du contrôle :

(1) Le système compile les dossiers de vérification des [*Affectation : composantes de système définies par l'organisation*] en une piste de vérification (logique ou physique) globale et établit une corrélation chronologique [*Affectation : niveau de tolérance défini par l'organisation des relations entre les timbres horodateurs des dossiers individuels de la piste de vérification*].

Conseils supplémentaires d'amélioration : Il y a corrélation chronologique de la piste de vérification lorsque le timbre horodateur des dossiers de vérification individuels peut être associé de manière fiable au timbre horodateur d'autres dossiers pour permettre un classement chronologique des dossiers à l'intérieur des limites de tolérance définies par l'organisation.

(2) Le système produit une piste de vérification (logique ou physique) globale composée de dossiers de vérification dont le format est normalisé.

Conseils supplémentaires d'amélioration : La normalisation de l'information de vérification en un format commun standard facilite l'interopérabilité et l'échange d'information entre des dispositifs et des systèmes d'information dissimilaires. Elle permet au système de vérification de produire sur les événements de l'information qu'il est plus facile d'analyser et de mettre en corrélation. Les dossiers des journaux système et les dossiers de vérification conformes à la norme CEE (Common Event Expression) sont des exemples de formats standard de dossier de vérification. Dans le cas des mécanismes de journalisation individuels du système qui ne respectent pas un format standard, le système peut convertir chaque dossier de vérification dans un format standard lors de la compilation de la piste de vérification globale.

Références :

Aucune.

AU-13 SURVEILLANCE DE LA DIVULGATION D'INFORMATION

Contrôle :

(A) L'organisation surveille l'information de source ouverte pour détecter toute exfiltration ou divulgation non autorisées d'information organisationnelle [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Aucune.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

AU-14 VÉRIFICATION DES SESSIONS

Contrôle :

(A) Le système d'information permet de saisir et (ou) d'enregistrer et de journaliser tout le contenu d'une session d'utilisateur.

(B) Le système d'information permet d'afficher et (ou) d'écouter à distance et en temps réel tout le contenu d'une session lancée par un utilisateur.

Conseils supplémentaires : Les activités de vérification des sessions sont développées, intégrées et utilisées en consultation avec des conseillers juridiques, conformément aux lois du GC et aux politiques, directives et normes concernées du SCT.

Améliorations du contrôle :

(1) Le système lance les vérifications de session au démarrage du système.

Références :

Aucune.

4.4 FAMILLE : ÉVALUATION ET AUTORISATION DE LA SÉCURITÉ

CLASSE : GESTION

CA-1 POLITIQUE ET PROCÉDURES D'ÉVALUATION ET D'AUTORISATION DE LA SÉCURITÉ

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des politiques d'évaluation et d'autorisation de la sécurité formelles et documentées qui définissent les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique d'évaluation et d'autorisation de la sécurité et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles d'évaluation et d'autorisation de la sécurité. Les politiques et procédures sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. Les politiques d'évaluation et d'autorisation de la sécurité peuvent être incluses dans la politique générale de sécurité de l'information de l'organisation. Les procédures d'évaluation et d'autorisation de la sécurité peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique d'évaluation et d'autorisation de la sécurité. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].
Directive sur la gestion de la sécurité ministérielle du SCT [Référence 11].

CA-2 ÉVALUATIONS DE LA SÉCURITÉ

Contrôle :

(A) L'organisation développe un plan d'évaluation de la sécurité qui décrit la portée de l'évaluation, incluant ce qui suit :

(a) Contrôles de sécurité et améliorations de contrôle sous évaluation;

(b) Procédures d'évaluation servant à déterminer l'efficacité des contrôles de sécurité; et

(c) Environnement d'évaluation, équipe d'évaluation et rôles et responsabilités liés à l'évaluation.

(B) L'organisation évalue les contrôles de sécurité du système d'information [*Affectation : fréquence définie par l'organisation*] pour déterminer la mesure dans laquelle ils sont appliqués correctement, fonctionnent

tel que prévu et produisent les résultats souhaités dans le respect des exigences relatives au contrôle de sécurité des systèmes.

(C) L'organisation produit un rapport d'évaluation de la sécurité qui documente les résultats de l'évaluation.

(D) L'organisation remet, par écrit, les résultats de l'évaluation à l'agent d'autorisation ou à un représentant désigné.

Conseils supplémentaires : L'organisation évalue les contrôles de sécurité du système d'information dans le contexte (i) de l'autorisation ou de la réautorisation de la sécurité, (ii) du respect des exigences du SCT relativement aux évaluations périodiques stipulées dans la *Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information* [Référence 8], (iii) de la surveillance permanente de la sécurité et (iv) des tests et des évaluations prévus dans le processus du cycle de développement des systèmes. Le rapport d'évaluation documente les résultats à un niveau que l'organisation juge suffisamment détaillé pour lui permettre d'en déterminer l'exactitude et l'exhaustivité et d'établir la mesure dans laquelle les contrôles sont appliqués correctement, fonctionnent tel que prévu et produisent les résultats souhaités dans le respect des exigences relatives au contrôle de sécurité des systèmes. Les organisations ne doivent pas percevoir les exigences du SCT relativement aux évaluations périodiques de la sécurité comme des exigences supplémentaires à celles déjà prévues dans le processus d'autorisation de sécurité. Pour satisfaire à ces exigences, elles peuvent utiliser les résultats de l'évaluation des contrôles de sécurité de l'une ou l'autre des sources qui suivent, incluant, sans s'y limiter : (i) les évaluations effectuées dans le cadre du processus d'autorisation ou de réautorisation des systèmes d'information; (ii) les activités de surveillance permanente (voir le contrôle CA-7); ou (iii) les tests et les évaluations prévus dans le processus du cycle de développement des systèmes (pour autant que les résultats soient actuels et pertinents pour la détermination de l'efficacité des contrôles de sécurité). On peut réutiliser les résultats existants de l'évaluation des contrôles dans la mesure où ils demeurent valables et sont complétés, au besoin, par des évaluations supplémentaires.

Après l'autorisation initiale du système d'information, en conformité avec la politique du SCT, l'organisation évalue périodiquement un sous-ensemble des contrôles de sécurité dans le cadre des activités de surveillance permanente. Elle établit les critères de sélection des contrôles puis en choisit, aux fins d'évaluation, un sous-ensemble dans le système d'information et son environnement d'exploitation. Les contrôles les plus volatiles (c.-à-d., ceux sur lesquels les changements constants apportés au système, ou à son environnement d'exploitation, ont le plus d'incidence) ou jugés critiques par l'organisation pour la protection des systèmes sont évalués plus fréquemment, en conformité avec l'évaluation des risques qu'elle privilégie. Tous les autres contrôles sont évalués au moins une fois durant le cycle d'autorisation du système d'information. À cette fin, l'organisation peut utiliser les résultats des évaluations mentionnées précédemment en autant qu'ils sont actuels, valables et pertinents pour la détermination de l'efficacité des contrôles. Les vérifications externes (p. ex., celles effectuées par des entités extérieures, tels les organismes réglementaires) sont hors de la portée de ce contrôle. Contrôles connexes : CA-6, CA-7, PM-9, SA-11.

Améliorations du contrôle :

(1) L'organisation utilise une équipe d'évaluation ou un évaluateur indépendant pour évaluer les contrôles de sécurité du système d'information.

Conseils supplémentaires d'amélioration : Une équipe d'évaluation ou un évaluateur indépendant est tout groupe ou individu capable d'effectuer une évaluation impartiale d'un système d'information organisationnel. Le terme évaluation impartiale signifie qu'il ne doit pas y avoir de conflit d'intérêt, perçu ou réel, entre les évaluateurs et les chaînes de développement, d'exploitation et (ou) de gestion du système ou la détermination de l'efficacité des contrôles de sécurité. Les services indépendants d'évaluation de la sécurité peuvent être assurés par d'autres éléments de l'organisation ou par des entités contractuelles du secteur public ou privé. Les services d'évaluation contractuels sont jugés indépendants lorsque le propriétaire du système ne participe pas directement au processus d'attribution du contrat ou ne peut influencer indûment l'impartialité de l'évaluateur ou de l'équipe d'évaluation. L'agent d'autorisation détermine le niveau requis d'indépendance de l'évaluateur selon les catégories de sécurité du système et (ou) le risque éventuel auquel peuvent être exposés les individus et les activités et les biens de l'organisation. Il établit si ce niveau d'indépendance est suffisant pour que l'organisation puisse avoir confiance que les résultats de l'évaluation sont fiables et peuvent servir à prendre des décisions crédibles concernant les risques. Dans certaines situations spéciales, par exemple lorsque le propriétaire du

système est une petite organisation ou que la structure organisationnelle fait en sorte que l'évaluation doit être effectuée par des individus qui sont partie prenante des chaînes de développement, d'exploitation et (ou) de gestion du système, l'indépendance du processus d'évaluation peut être garantie par une analyse et un examen minutieux des résultats de l'évaluation confiés à une équipe d'experts indépendants qui attesteront de l'exhaustivité, de l'exactitude de l'intégrité et de la fiabilité des résultats.

(2) L'organisation intègre aux évaluations des contrôles de sécurité, [*Affectation : fréquence définie par l'organisation*], [*Sélection : avec préavis, sans préavis*], [*Sélection : surveillance en profondeur; test de détection d'utilisateur malveillant; test de pénétration; exercices de l'équipe d'intervention; [Affectation : autres formes de test de sécurité définies par l'organisation]*].

Conseils supplémentaires d'amélioration : Les tests de pénétration exercent des contrôles de sécurité à la fois physiques et techniques. La méthode standard d'application de ces tests inclut ce qui suit : (i) analyse pré-test basée sur une connaissance détaillée du système cible, (ii) identification pré-test des vulnérabilités potentielles basée sur l'analyse pré-test et (iii) tests conçus pour déterminer l'exploitabilité des vulnérabilités identifiées. Toutes les parties doivent convenir des règles détaillées d'engagement avant le début de tout scénario de test de pénétration. Il faut établir une corrélation entre ces règles et les outils, techniques et procédures dont on prévoit l'utilisation par les sources de menaces qui lanceront les attaques. Une évaluation organisationnelle des risques permet de décider du niveau d'indépendance exigé des agents ou des équipes chargés des tests de pénétration. Les exercices de l'équipe d'intervention sont menés de manière à simuler une tentative conflictuelle de compromission des missions et (ou) des processus opérationnels de l'organisation qui permet d'évaluer en détail la capacité du système et de l'organisation en matière de protection de la sécurité de l'information. Les tests de pénétration peuvent être effectués en laboratoire. Quant aux exercices de l'équipe d'intervention, leur portée est plus étendue et vise à créer des conditions réelles d'exploitation. La surveillance du système d'information, les tests de détection d'utilisateur malveillant, les tests de pénétration, les exercices de l'équipe d'intervention et autres formes de tests de sécurité (p. ex., vérification et validation indépendantes) visent à améliorer l'état de préparation de l'organisation en faisant appel à ses capacités d'intervention; ils permettent de déterminer les niveaux actuels de rendement de l'organisation comme moyens de cibler ses interventions et d'améliorer son état de sécurité et celui du système. Les méthodes de test sont approuvées par les agents d'autorisation, en conformité avec la stratégie de gestion du risque de l'organisation. Les vulnérabilités relevées durant les exercices de l'équipe d'intervention sont intégrées au processus de corrections des vulnérabilités. Contrôles connexes : RA-5, SI-2.

Références :

Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].
Directive sur la gestion de la sécurité ministérielle du SCT [Référence 11].

CA-3 CONNEXIONS DES SYSTÈMES D'INFORMATION

Contrôle :

(A) L'organisation autorise les connexions du système d'information à d'autres systèmes sur lesquels elle n'a aucune autorité en recourant à des ententes sur la sécurité des interconnexions.

(B) L'organisation documente, pour chaque connexion, les caractéristiques d'interface, les exigences des contrôles de sécurité et la nature de l'information communiquée.

(C) L'organisation surveille en permanence les connexions du système d'information et vérifie le respect des exigences en matière de contrôle de sécurité.

Conseils supplémentaires : Ce contrôle s'applique aux connexions spécialisées entre les systèmes d'information et non aux connexions temporaires contrôlées par les utilisateurs, tel le courrier électronique et la navigation dans les sites Web. L'organisation évalue méticuleusement les risques possibles liés à l'interconnexion de systèmes d'information, tant intérieurs qu'extérieurs, dont les exigences de contrôle de sécurité et les contrôles eux-mêmes diffèrent. Les agents d'autorisation déterminent les risques associés à chaque connexion ainsi que les contrôles appropriés qui doivent être utilisés. Si l'agent d'autorisation des systèmes interconnectés est le même, aucune entente sur la sécurité des interconnexions n'est requise; les caractéristiques d'interface entre les systèmes sont alors décrits dans les plans de sécurité de chaque système. Si l'agent d'autorisation est différent pour chaque système et appartient à la même organisation, soit cette dernière détermine s'il y a lieu de conclure une entente, soit les caractéristiques d'interface entre les systèmes sont décrits dans les plans de sécurité de chaque système.

Plutôt que de développer une entente, les organisations peuvent choisir d'intégrer cette information à un contrat formel, plus particulièrement lorsque l'interconnexion est effectuée entre un ministère ou un organisme du GC et un organisme non gouvernemental (secteur privé). Dans tous les cas, on doit documenter les caractéristiques d'interface; toutefois, les formalités et le processus d'approbation peuvent varier considérablement même s'ils visent un objectif fondamental similaire, soit gérer les risques liés à l'interconnexion des systèmes. Les risques concernent également les systèmes qui partagent les mêmes réseaux. Les systèmes peuvent être des dispositifs et doivent être identifiés et authentifiés comme tels, en conformité avec le contrôle IA-3. Contrôles connexes : AC-4, IA-3, SC-7, SA-9.

Améliorations du contrôle :

(1) L'organisation interdit toute connexion directe d'un système non classifié, essentiel à la sécurité nationale, à un réseau externe.

Conseils supplémentaires d'amélioration : Un réseau externe est un réseau qui échappe au contrôle de l'organisation (p. ex., Internet). L'interdiction de connexion directe signifie qu'un système ne peut se connecter à un réseau externe sans utiliser un dispositif approuvé de protection des frontières (p. ex., pare-feu) qui négocie les communications entre le système et le réseau.

(2) L'organisation interdit toute connexion directe d'un système classifié, essentiel à la sécurité nationale, à un réseau externe.

Conseils supplémentaires d'amélioration : Un réseau externe est un réseau qui échappe au contrôle de l'organisation (p. ex., Internet). L'interdiction de connexion directe signifie qu'un système ne peut se connecter à un réseau externe sans utiliser un dispositif approuvé de protection des frontières (p. ex., pare-feu) qui négocie les communications entre le système et le réseau. En plus, le dispositif approuvé (normalement un système inter-domaine doté d'une interface gérée) applique les règles de flux d'information entre le système et le réseau externe, en conformité avec le contrôle AC-4.

Références :

Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22) du CSTC [Référence 42].
Établissement des zones de sécurité dans un réseau – Considérations en matière de positionnement des services au sein de zones spécifiques (ITSG-38) du CSTC [Référence 44].

CA-4 CERTIFICATION DE LA SÉCURITÉ

[Annulé : Intégré au contrôle CA-2].

CA-5 PLAN DE MISE EN ŒUVRE DES MESURES DE PROTECTION (PLAN D'ACTION ET JALONS)

Contrôle :

(A) L'organisation développe un plan d'action et des jalons pour le système d'information afin de documenter les mesures correctives qu'elle prévoit utiliser pour corriger les faiblesses ou les lacunes relevées durant l'évaluation des contrôles de sécurité et pour réduire et éliminer les vulnérabilités connues du système.

(B) L'organisation met à jour le plan d'action et les jalons existants [*Affectation : fréquence définie par l'organisation*] en tenant compte des constatations des évaluations de contrôles de sécurité, des analyses des répercussions sur la sécurité et des activités de surveillance permanente.

Conseils supplémentaires : Le plan d'action et les jalons sont une section du plan de sécurité des opérations, document clé de la trousse d'autorisation de la sécurité qui peut être assujetti aux exigences de déclaration de l'organisation et du GC. Contrôle connexe : PM-4.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour s'assurer que le plan d'action et les jalons du système sont exacts, à jour et facilement accessibles.

Références :

Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8]. *Annexe 2 du Guide de gestion des risques de sécurité des systèmes d'information – Processus de mise en œuvre de la sécurité de l'information (ITSG-33) du CSTC* [Référence 60].

CA-6 AUTORISATION DE SÉCURITÉ

Contrôle :

(A) L'organisation attribue à un cadre supérieur ou à un gestionnaire le rôle d'agent d'autorisation du système d'information.

(B) L'organisation s'assure que l'agent autorise le système d'information aux fins de traitement avant d'en commencer l'exploitation.

(C) L'organisation met à jour l'autorisation de sécurité [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : L'autorisation de sécurité est la décision de gestion officielle, communiquée dans un document de décision d'autorisation par un cadre supérieur (c.-à-d., l'agent d'autorisation), qui autorise l'exploitation d'un système d'information et confirme que les responsables acceptent explicitement les risques qui menacent les activités et les biens de l'organisation, les individus, les autres organisations et le Canada. Les agents d'autorisation supervisent normalement le budget des systèmes d'information ou sont responsable de la mission ou des activités opérationnelles prises en charge par ces systèmes. L'autorisation de sécurité est essentiellement une responsabilité gouvernementale et les agents d'autorisation doivent être des employés du gouvernement. Par ce processus d'autorisation, les agents sont responsables des risques de sécurité associés à l'exploitation du système. Ils occupent donc des postes de gestion dont le niveau d'autorité correspond à la compréhension et à l'acceptation de tels risques pour la sécurité. Le recours à un processus continu et détaillé de surveillance leur permet de tenir à jour en permanence l'information essentielle contenue dans la trousse d'autorisation (c.-à-d., le plan de sécurité (incluant l'évaluation des risques), le rapport d'évaluation de la sécurité et le plan d'action et les jalons) et de fournir au propriétaire du système un aperçu à jour de l'état de sa sécurité. Pour réduire les coûts administratifs associés aux nouvelles autorisations de sécurité, l'agent utilise le plus possible les résultats du processus de surveillance permanente comme base des décisions concernant ces autorisations. Les organisations doivent effectuer périodiquement de nouvelles autorisations des systèmes d'information, tel que stipulé par le SCT et les règlements de l'organisation, ou lorsque qu'une modification importante est apportée au système. L'organisation définit ce qui constitue une modification importante. Contrôles connexes : CA-2, CA-7, PM-9, PM-10.

Améliorations du contrôle :

Aucune.

Références :

Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8]. *Directive sur la gestion de la sécurité ministérielle du SCT* [Référence 11].

CA-7 SURVEILLANCE PERMANENTE

Contrôle :

(A) L'organisation développe une stratégie de surveillance permanente et met en œuvre un programme de surveillance permanente qui inclut un processus de gestion de la configuration du système d'information et de ses composantes.

(B) L'organisation développe une stratégie de surveillance permanente et met en œuvre un programme de surveillance permanente qui inclut une détermination, au plan de la sécurité, de l'incidence des modifications apportées au système d'information et à l'environnement d'exploitation.

(C) L'organisation développe une stratégie de surveillance permanente et met en œuvre un programme de surveillance permanente qui inclut des évaluations permanentes des contrôles de sécurité, en conformité avec sa stratégie de surveillance permanente.

(D) L'organisation développe une stratégie de surveillance permanente et met en œuvre un programme de surveillance permanente qui inclut la déclaration de l'état de sécurité du système d'information aux agents concernés de l'organisation [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Un programme de surveillance permanente permet à l'organisation de maintenir en permanence l'autorisation de sécurité d'un système dans un environnement d'exploitation très dynamique où les menaces, les vulnérabilités, les technologies et les missions et (ou) processus opérationnels sont en constante évolution. La surveillance permanente des contrôles de sécurité effectués avec des outils de soutien automatisés facilite la gestion quasi en temps réel des risques et favorise la sensibilisation à la situation de l'organisation concernant l'état de sécurité du système. La mise en œuvre de ce type de programme permet la tenue à jour permanente du plan de sécurité, des rapports d'évaluation et des autres documents clés de la trousse d'autorisation de la sécurité. Un programme de surveillance permanente rigoureux et bien exécuté réduit de manière significative le niveau d'effort requis pour la réautorisation du système d'information. Les activités de surveillance sont adaptées aux catégories de sécurité des systèmes. Contrôles connexes : CA-2, CA-5, CA-6, CM-3, CM-4.

Améliorations du contrôle :

(1) L'organisation fait appel à une équipe d'évaluation ou un évaluateur indépendant pour surveiller en permanence les contrôles de sécurité du système d'information.

Conseils supplémentaires d'amélioration : L'organisation peut étendre et maximiser la valeur de l'évaluation permanente des contrôles de sécurité durant le processus de surveillance en exigeant de l'équipe d'évaluation ou de l'évaluateur indépendant qu'ils évaluent tous les contrôles de sécurité durant la période d'autorisation du système. Voir les conseils supplémentaires du contrôle CA-2, amélioration (1), pour plus d'information sur l'indépendance de l'évaluateur. Contrôles connexes : CA-2, CA-5, CA-6, CM-4.

(2) L'organisation prévoit, planifie et effectue les évaluations [*Affectation : fréquence définie par l'organisation*], [*Sélection : avec préavis, sans préavis*], [*Sélection : surveillance en profondeur; test de détection d'utilisateur malveillant; test de pénétration; exercices de l'équipe d'intervention; [Affectation : autres formes de test de sécurité définies par l'organisation]*] pour assurer la conformité à toutes les procédures d'atténuation des vulnérabilités.

Conseils supplémentaires d'amélioration : Vous trouverez des exemples de procédures d'atténuation des vulnérabilités dans les alertes de sécurité. Les tests visent à s'assurer que le système continue d'offrir une protection adéquate contre des menaces et des vulnérabilités en constante évolution. Les tests de conformité offrent également une validation indépendante. Voir les conseils supplémentaires du contrôle CA-2, amélioration (2), pour plus de détails sur les tests de détection d'utilisateur malveillant, les tests de pénétration, les exercices de l'équipe d'intervention et les autres formes de test de sécurité. Contrôle connexe : CA-2.

Références :

Directive sur la gestion de la sécurité ministérielle du SCT [Référence 11].

4.5 FAMILLE : GESTION DE LA CONFIGURATION

CLASSE : OPÉRATIONNELLE

CM-1 POLITIQUE ET PROCÉDURES DE GESTION DE LA CONFIGURATION

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique de gestion de la configuration formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de gestion de la configuration et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de gestion de la configuration. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique de gestion de la configuration peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures de gestion de la configuration peuvent être développées pour le programme de sécurité général (ou programme des TI) et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique de gestion de la configuration. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].

CM-2 CONFIGURATION DE BASE

Contrôle :

(A) L'organisation développe, documente et tient à jour la configuration de base actuelle du système d'information.

Conseils supplémentaires : Ce contrôle établit la configuration de base du système d'information et de ses composantes, y compris les communications et les éléments de connectivité. La configuration de base donne de l'information sur les composantes (p. ex., logiciel standard de poste de travail, serveur, composante réseau ou dispositif mobile, incluant le système d'exploitation et les applications installées ainsi que les numéros de version et de l'information sur les rustines), la topologie du réseau et l'emplacement logique des composantes dans l'architecture du système. La configuration est une spécification documentée et à jour sur laquelle repose tout le système d'information. Sa tenue à jour requiert la création de nouvelles bases au fur et à mesure de l'évolution

du système. La configuration de base est conforme à l'architecture d'entreprise de l'organisation. Contrôles connexes : CM-3, CM-6, CM-8, CM-9.

Améliorations du contrôle :

(1) L'organisation examine et met à jour la configuration de base du système d'information :

(a) [*Affectation : fréquence définie par l'organisation*];

(b) Le cas échéant, [*Affectation : circonstances définies par l'organisation*]; et

(c) Dans le cadre des installations et des mises à niveau des composantes du système d'information.

(2) L'organisation utilise des mécanismes automatisés pour assurer le maintien d'une configuration de base à jour, complète, précise et facilement accessible.

Conseils supplémentaires d'amélioration : Les outils d'inventaire de logiciel sont des exemples de mécanismes automatisés qui aident les organisations à maintenir l'uniformité de leurs configurations de base. Ils peuvent être déployés pour chaque système d'exploitation utilisé dans l'organisation (p. ex., postes de travail, serveurs, composantes réseau, dispositifs mobiles) et servir à pister les numéros de version, les applications et les types de logiciel installés des systèmes d'exploitation ainsi que les niveaux des rustines actuelles. Ils peuvent également analyser les systèmes d'information afin de repérer tout logiciel non autorisé et de valider les listes des programmes autorisés et non autorisés définies par l'organisation.

(3) L'organisation conserve les anciennes versions des configurations de base lorsqu'elle le juge nécessaire pour permettre le retour à la version précédente.

(4) L'organisation :

(a) Développe et maintient [*Affectation : liste définie par l'organisation des programmes qui ne peuvent être exécutés dans le système*]; et

(b) Utilise une politique d'autorisation (tout permettre, interdire par exception) pour identifier le logiciel qui peut être exécuté dans le système d'information.

(5) L'organisation :

(a) Développe et maintient [*Affectation : liste définie par l'organisation des programmes qui peuvent être exécutés dans le système*]; et

(b) Utilise une politique d'autorisation (tout interdire, permettre par exception) pour identifier le logiciel qui peut être exécuté dans le système d'information.

(6) L'organisation maintient pour les environnements de développement et de test une configuration de base gérée séparément de la configuration opérationnelle.

Références :

Aucune.

CM-3 CONTRÔLE DES MODIFICATIONS DE LA CONFIGURATION

Contrôle :

(A) L'organisation détermine les types de modification du système d'information qui sont liés à la configuration.

(B) L'organisation approuve les modifications liées à la configuration en tenant compte explicitement des analyses des répercussions sur la sécurité.

(C) L'organisation documente les modifications approuvées liées à la configuration.

(D) L'organisation conserve et examine les dossiers des modifications liées à la configuration.

(E) L'organisation vérifie les activités relatives aux modifications liées à la configuration.

(F) L'organisation coordonne et surveille les activités de contrôle des modifications de la configuration par [*Affectation : élément de contrôle des modifications de la configuration défini par l'organisation (p. ex., comité, conseil*] qui se réunit [*Sélection : (une ou plusieurs): [Affectation : fréquence définie par l'organisation]; [Affectation : conditions de modification de la configuration définies par l'organisation]*].

Conseils supplémentaires : L'organisation détermine les types de modification liés à la configuration. Le contrôle des modifications inclut la proposition systématique, la justification, la mise en œuvre, les tests et (ou) l'évaluation, l'examen et l'utilisation des modifications, incluant les mises à niveau. Il inclut les modifications des composantes, des paramètres de configuration des produits de technologie de l'information (p. ex., systèmes d'exploitation, applications, pare-feu, routeurs), les modifications d'urgence et celles servant à corriger des lacunes. Un processus organisationnel type de gestion des modifications de la configuration inclut, par exemple, un comité reconnu de gestion de la configuration qui approuve les modifications. La vérification des modifications inclut les activités effectuées avant et après la modification et les activités de vérification nécessaires à sa mise en œuvre. Contrôles connexes : CM-4, CM-5, CM-6, SI-2.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour :

(a) Documenter les modifications proposées au système d'information;

(b) Informer les autorités d'approbation désignées;

(c) Souligner les approbations qui n'ont pas été reçues le ou avant le [*Affectation : durée définie par l'organisation*];

(d) Retenir les modifications jusqu'à la réception des approbations des autorités désignées; et

(e) Documenter les modifications qui ont été effectuées.

(2) L'organisation teste, valide et documente les modifications avant de les inclure dans le système opérationnel.

Conseils supplémentaires d'amélioration : L'organisation s'assure que les tests ne nuisent pas aux opérations du système d'information. L'individu et (ou) le groupe chargé des tests comprend les politiques et les procédures de sécurité de l'organisation, les politiques et les procédures du système d'information et les risques pour la santé, la sécurité et l'environnement associés à une installation et (ou) un processus spécifique. Il peut arriver que l'on doive mettre hors ligne un système en production, ou le dupliquer dans la mesure du possible, avant de pouvoir effectuer les tests. Si un système doit être mis hors ligne, on doit faire le maximum pour que ce soit durant une période prévue d'interruption. Dans les cas où l'organisation ne peut effectuer ces tests sur un système en production, elle utilise des contrôles de compensation (p. ex., fournir une copie du système) en conformité avec les directives de personnalisation.

(3) L'organisation utilise des mécanismes automatisés pour apporter les modifications au système de base actuel et les déploie ensuite dans l'ensemble des systèmes installés.

Conseils supplémentaires d'amélioration : Contrôles connexes : CM-2, CM-6.

(4) L'organisation exige qu'un représentant de la sécurité de l'information soit membre de [*Affectation : élément de contrôle des modifications de la configuration (p. ex., comité, conseil) défini par l'organisation*].

Conseils supplémentaires d'amélioration : Les représentants de la sécurité de l'information peuvent inclure, par exemple, des agents de sécurité de système d'information ou des gestionnaires de la sécurité des systèmes d'information. L'élément de contrôle des modifications de la configuration de cette amélioration est conforme à celui défini par l'organisation dans le contrôle CM-3.

Références :

Aucune.

CM-4 ANALYSE DES RÉPERCUSSIONS SUR LA SÉCURITÉ

Contrôle :

(A) L'organisation analyse, avant de les mettre en œuvre, les modifications apportées au système d'information pour déterminer leurs éventuelles répercussions sur la sécurité.

Conseils supplémentaires : Les analyses des répercussions sont effectuées par le personnel de l'organisation responsable de la sécurité de l'information, incluant, par exemple, les administrateurs de système d'information, les agents de la sécurité des systèmes d'information, les gestionnaires de la sécurité des systèmes d'information et les techniciens en sécurité des systèmes d'information. Ces employés possèdent les compétences appropriées et l'expertise technique nécessaires pour analyser les modifications et leurs ramifications au plan de la sécurité. L'analyse peut inclure, par exemple, l'examen de la documentation du système, tel le plan de sécurité, pour comprendre la façon dont sont appliqués certains contrôles de sécurité et les répercussions possibles des modifications qui leur sont apportées. Elle peut également inclure une évaluation des risques pour bien saisir l'incidence des modifications et déterminer si des contrôles de sécurité supplémentaires sont requis. L'analyse des répercussions est adaptée à la catégorie de sécurité du système d'information. Contrôles connexes : CA-2, CA-7, CM-3, CM-9, SI-2.

Améliorations du contrôle :

(1) L'organisation analyse les nouveaux logiciels dans un environnement de test distinct avant de les installer dans un environnement opérationnel afin de déceler toute lacune, faiblesse, incompatibilité ou intention malveillante susceptible d'influer sur la sécurité.

(2) L'organisation, après que les modifications ont été apportées au système, vérifie les fonctions de sécurité pour s'assurer qu'elles ont été mise en œuvre correctement, qu'elles fonctionnent tel que prévu et qu'elles produisent les résultats souhaités, conformément aux exigences du contrôle de la sécurité des systèmes.

Conseils supplémentaires d'amélioration : Les modifications incluent à la fois les modifications et les mises à niveau du système.

Références :

Aucune.

CM-5 RESTRICTIONS D'ACCÈS ASSOCIÉES AUX MODIFICATIONS

Contrôle :

(A) L'organisation définit, documente, approuve et applique les restrictions d'accès logique et physique associées aux modifications du système d'information.

Conseils supplémentaires : Les modifications des composantes matérielles, logicielles et (ou) micrologicielles du système d'information peuvent avoir des effets importants sur la sécurité globale du système. Seules des personnes qualifiées et autorisées peuvent donc obtenir l'accès aux composantes du système pour effectuer des modifications, incluant les mises à niveau. En plus, il est important de tenir à jour des dossiers d'accès pour s'assurer que le contrôle des modifications de la configuration est appliqué de la manière prévue et pour appuyer les interventions après le fait dans l'éventualité où l'organisation détecte une modification non autorisée. Les restrictions d'accès associées aux modifications incluent également les bibliothèques de logiciel. Les exemples de restrictions d'accès incluent les contrôles d'accès physique et logique (voir les contrôles AC-3 et PE-3), l'automatisation des flux de travail, les bibliothèques de soutien, les couches abstraites (p. ex., des modifications apportées à l'interface d'une tierce partie plutôt que directement à la composante du système) et les fenêtres de modification (p. ex., modifications autorisées seulement à des moments spécifiques, ce qui permet de repérer facilement les modifications non autorisées). Certains mécanismes et processus d'application nécessaires à la mise en œuvre de ce contrôle de sécurité sont inclus dans d'autres contrôles. Dans le cas des mesures appliquées

par ces autres contrôles, le présent contrôle fournit l'information requise pour leur permettre de répondre à leur besoins spécifiques, soit autoriser les modifications du système, vérifier les modifications et assurer la mise à jour et l'examen des dossiers des modifications. Contrôles connexes : AC-3, AC-6, PE-3.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour appliquer les restrictions d'accès et faciliter la vérification des mesures d'application.

(2) L'organisation vérifie les modifications apportées au système d'information [*Affectation : fréquence définie par l'organisation*] et, le cas échéant, détermine s'il y a eu des modifications non autorisées.

(3) Le système empêche l'installation de [*Affectation : programmes logiciels critiques définis par l'organisation*] qui ne portent pas la signature d'un certificat reconnu et approuvé par l'organisation.

Conseils supplémentaires d'amélioration : Les programmes et (ou) modules critiques incluent, par exemple, les rustines, les service packs et, le cas échéant, les pilotes de dispositif.

(4) L'organisation applique la règle des deux personnes pour les modifications de [*Affectation : information système et composantes de système définies par l'organisation*].

(5) L'organisation :

(a) Restreint les privilèges accordés aux développeurs et (ou) aux intégrateurs de système pour ce qui touche les modifications, directement dans l'environnement de production, des composantes matérielles, logicielles et micrologicielles et du système d'information; et

(b) Examine et réévalue les privilèges accordés aux développeurs et (ou) aux intégrateurs de système [*Affectation : fréquence définie par l'organisation*].

(6) L'organisation restreint les privilèges de modification du logiciel inclut dans les bibliothèques de logiciel (incluant les programmes privilégiés).

(7) Le système applique automatiquement [*Affectation : mesures de protection et contremesures définies par l'organisation*] lorsque les fonctions (ou mécanismes) de sécurité sont modifiées de manière inappropriée.

Conseils supplémentaires d'amélioration : Le système réagit automatiquement lorsque les fonctions (ou mécanismes) de sécurité sont modifiées de manière inappropriée et (ou) non autorisée. L'application automatique des mesures de protection et des contremesures inclut, par exemple, l'annulation de la modification, l'interruption du système ou le déclenchement d'une alerte sonore dès que se produit une modification non autorisée d'un fichier de sécurité critique.

Références :

Aucune.

CM-6 PARAMÈTRES DE CONFIGURATION

Contrôle :

(A) L'organisation établit et documente les paramètres obligatoires de configuration des produits de technologie de l'information intégrés au système d'information en utilisant des [*Affectation : listes de vérification de la sécurité de la configuration définies par l'organisation*] qui incluent les restrictions les plus strictes stipulées dans les exigences opérationnelles.

(B) L'organisation applique les paramètres de configuration.

(C) L'organisation identifie, documente et approuve les exceptions aux paramètres obligatoires de configuration des composantes individuelles en tenant compte d'exigences opérationnelles explicites.

(D) L'organisation surveille et contrôle les modifications des paramètres de configuration en conformité avec ses politiques et procédures.

Conseils supplémentaires : Les paramètres de configuration sont les paramètres de sécurité configurables des produits de technologie de l'information intégrés au système d'information. Ils ont une incidence sur l'état de sécurité du système et incluent les paramètres qui servent à satisfaire aux autres exigences de contrôle de la sécurité. Ils incluent, par exemple, les paramètres de registre, de comptes, de fichiers et d'annuaires (c.-à-d., les permissions) ainsi que les paramètres de services, de ports, de protocoles et de connexion à distance. Les organisations définissent des paramètres de configuration obligatoires qui servent à configurer les paramètres des systèmes individuels. La liste de vérification de configuration de la sécurité (parfois appelée guide de verrouillage, guide de renforcement, guide de sécurité, guide technique de mise en œuvre de la sécurité (STIG), ou repère) inclut une suite d'instructions ou de procédures qui permettent de répondre aux exigences opérationnelles relatives à la configuration des composantes de système. Les listes de vérification peuvent être développées par des fournisseurs et des développeurs de technologie de l'information, des consortiums, le milieu universitaire, l'industrie, des organismes fédéraux et autres organisations des secteurs public et privé. Le protocole SCAP (Security Content Automation Protocol) et les normes qu'il définit (p. ex., la norme CCE (Common Configuration Enumeration)) offrent une méthode efficace d'identification unique, de pistage et de contrôle des paramètres de configuration. Contrôles connexes : CM-2, CM-3, SI-4.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour centraliser la gestion, l'application et la vérification des paramètres de configuration.

(2) L'organisation utilise des mécanismes automatisés pour intervenir en cas de modification non autorisée des [*Affectation : paramètres définis par l'organisation de configuration*].

Conseils supplémentaires d'amélioration : Les interventions en cas de modification non autorisée des paramètres de configuration peuvent inclure, par exemple, l'alerte du personnel désigné de l'organisation, la restauration des paramètres de configuration obligatoires et (ou) définis par l'organisation ou, dans des cas extrêmes, l'interruption de traitement du système en cause.

(3) L'organisation intègre un mécanisme de détection des modifications non autorisées de la configuration à sa capacité d'intervention en cas d'incident pour s'assurer de pister, surveiller, corriger et conserver à des fins historiques les événements concernés.

Conseils supplémentaires d'amélioration : Contrôles connexes : IR-4, IR-5.

(4) Le système (et les modifications apportées à la configuration de base) doit démontrer qu'il se conforme aux directives de configuration de la sécurité (c.-à-d., les listes de vérification de la sécurité) avant d'être déployé dans l'environnement de production.

Références :

Sécurité de base recommandée pour Windows Serveur 2003 (ITSG-20) du CSTC [Référence 41].
Isolation d'un serveur d'entreprise Blackberry dans un environnement Microsoft Exchange (ITSG-23) du CSTC [Référence 43].

CM-7 FONCTIONNALITÉ MINIMALE

Contrôle :

(A) L'organisation configure le système d'information de manière à offrir uniquement les capacités jugées essentielles et interdit ou restreint spécifiquement l'utilisation des fonctions, ports, protocoles et (ou) services suivants : [*Affectation : liste définie par l'organisation des fonctions, ports, protocoles et (ou) services interdits ou restreints*].

Conseils supplémentaires : Les systèmes d'information peuvent offrir une grande variété de fonctions et de services. Il peut arriver que des fonctions et des services fournis par défaut ne soient pas nécessaires au soutien des activités organisationnelles essentielles (p. ex., missions et fonctions clés). Dans la mesure du possible, les organisations limitent la fonctionnalité d'une composante à une seul fonction par dispositif (p. ex., serveur de

courrier, serveur Web, non les deux). Les fonctions et services fournis par les systèmes de l'organisation, ou par certaines de leurs composantes, doivent être examinés avec soin pour déterminer ceux qui peuvent être supprimés (p. ex., Voix sur IP, messagerie instantanée, auto-exécution, partage de fichiers). Les organisations doivent envisager de désactiver les ports physiques et logiques et les protocoles inutilisés ou non requis (p. ex., USB, FTP, IPv6, HTTP) des composantes pour éviter les connexions de dispositifs, les transferts d'information ou la tunnellisation non autorisés. Elles peuvent recourir à des outils d'analyse de réseau, des systèmes de détection et de prévention d'intrusions et à des mécanismes de protection de point terminal (pare-feu, système de détection d'intrusions intégré, etc.) pour identifier les fonctions, ports, protocoles et services interdits et en empêcher l'utilisation. Contrôle connexe : RA-5.

Améliorations du contrôle :

(1) L'organisation examine le système d'information [*Affectation : fréquence définie par l'organisation*] pour identifier et supprimer les fonctions, ports, protocoles et (ou) services non requis.

(2) L'organisation utilise des mécanismes automatisés pour empêcher l'exécution des programmes en conformité avec [*Sélection (une ou plusieurs): liste des programmes autorisés; liste des programmes non autorisés; règles d'autorisation des modalités d'utilisation d'un programme*].

Conseils supplémentaires d'amélioration : Contrôle connexe : CM-2.

(3) L'organisation assure le respect des [*Affectation : exigences d'enregistrement définies par l'organisation concernant les ports, protocoles et services*].

Conseils supplémentaires d'amélioration : Les organisations utilisent le processus d'enregistrement pour gérer, pister et surveiller les systèmes et les fonctions activées.

Références :

Aucune.

CM-8 INVENTAIRE DES COMPOSANTES DE SYSTÈME D'INFORMATION

Contrôle :

(A) L'organisation développe, documente et tient à jour un inventaire des composantes de système d'information qui reflète correctement le système d'information actuel.

(B) L'organisation développe, documente et tient à jour un inventaire des composantes de système d'information conforme à la limite d'autorisation du système d'information.

(C) L'organisation développe, documente et tient à jour un inventaire des composantes de système d'information au niveau de granularité jugé nécessaire pour permettre le suivi et la production de rapports.

(D) L'organisation développe, documente et tient à jour un inventaire des composantes de système d'information qui inclut [*Affectation : information définie par l'organisation et jugée nécessaire à la réalisation d'une comptabilisation efficace des immobilisations*].

(E) L'organisation développe, documente et tient à jour un inventaire des composantes de système d'information que les agents désignés de l'organisation peuvent examiner et vérifier.

Conseils supplémentaires : L'information que l'organisation juge nécessaire pour une comptabilisation efficace des immobilisations peut inclure, par exemple, les spécifications de l'inventaire du matériel (fabricant, type, modèle, numéro de série, emplacement physique), l'information sur les licences de logiciel, le propriétaire du système d'information et (ou) des composantes et, dans le cas des composantes ou des dispositifs réseau, le nom de la machine et l'adresse réseau. Contrôles connexes : CM-2, CM-6.

Améliorations du contrôle :

(1) L'organisation met à jour l'inventaire des composantes de système d'information dans le cadre des activités d'installation et de retrait des composantes et de mise à jour du système.

(2) L'organisation utilise des mécanismes automatisés pour faciliter la tenue à jour d'un inventaire de composantes à jour, complet, précis et facilement accessible.

Conseils supplémentaires d'amélioration : Les organisations tiennent à jour l'inventaire des systèmes d'information dans la mesure du possible. Il peut être difficile, par exemple, de surveiller les machines virtuelles car elles sont invisibles dans le réseau lorsqu'elles ne sont pas utilisées. Dans de tels cas, l'objectif de l'amélioration de contrôle est de maintenir un inventaire raisonnablement à jour, complet et précis.

(3) L'organisation :

(a) Utilise des mécanismes automatisés [*Affectation : fréquence définie par l'organisation*] pour détecter l'ajout de toute composante et (ou) de tout dispositif non autorisés au système d'information; et

(b) Désactive l'accès réseau de ces composantes et (ou) dispositifs ou informe les agents désignés de l'organisation.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle est appliquée en sus de la surveillance des connexions à distance non autorisées (contrôle AC-17) et des dispositifs mobiles non autorisés (contrôle AC-19). La surveillance des composantes et (ou) des dispositifs non autorisés dans les réseaux peut être effectuée en permanence ou lors des analyses périodiques des réseaux de l'organisation conçues à cet effet. Les mécanismes automatisés peuvent être appliqués dans le système lui-même et (ou) dans un système ou dispositif distinct. Contrôles connexes : AC-17, AC-19.

(4) L'organisation inclut, dans les données sur la comptabilité des biens, de l'information sur les composantes de système comme moyen d'identifier par [*Sélection (une valeur ou plus) : nom; poste; rôle*] les individus responsables de l'administration de ces composantes.

(5) L'organisation vérifie que toutes les composantes incluses dans la limite d'autorisation du système soit figurent dans l'inventaire du système, soit sont reconnues par autre système comme composante du système.

(6) L'organisation inclut dans l'inventaire des composantes les configurations de composantes évaluées et les déviations approuvées pour les configurations déjà déployées.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle concerne principalement les paramètres de configuration que l'organisation a définis pour ses composantes et les composantes spécifiques évaluées aux fins de conformité aux paramètres de configuration obligatoires, ainsi que tout écart approuvé des paramètres de configuration définis pour les composantes déployées. Contrôles connexes : CM-2, CM-6.

Références :

Aucune.

CM-9 PLAN DE GESTION DE LA CONFIGURATION

Contrôle :

(A) L'organisation développe, documente et met en œuvre pour le système d'information un plan de gestion de la configuration qui traite des rôles, des responsabilités et des processus et procédures de gestion de la configuration.

(B) L'organisation développe, documente et met en œuvre pour le système d'information un plan de gestion de la configuration qui définit les éléments de configuration du système et précise à quel moment les éléments sont gérés dans le cycle de développement des systèmes.

(C) L'organisation développe, documente et met en œuvre pour le système d'information un plan de gestion de la configuration qui définit les moyens d'identifier les éléments de configuration durant le cycle de développement des systèmes ainsi qu'un processus de gestion de leur configuration.

Conseils supplémentaires : Les éléments de configuration sont des éléments du système d'information (matériel, logiciel, micrologiciel et documentation) dont la configuration doit être gérée. Le plan de gestion de la configuration satisfait aux exigences de la politique de gestion de la configuration de l'organisation et est adapté au système individuel. Il définit en détail les processus et les procédures d'utilisation de la gestion de la configuration pour appuyer les activités du cycle de développement de chaque système. Le plan décrit la façon d'appliquer une modification dans le processus de gestion des modifications, de mettre à jour les paramètres et les éléments de base de la configuration, de tenir à jour l'inventaire des composantes, de contrôler les environnements de développement, de test et de production et, finalement, de développer, diffuser et mettre à jour les documents. Le processus d'approbation de la gestion de la configuration inclut la désignation des responsables de la gestion des clés chargés d'examiner et d'approuver les modifications proposées du système, et l'identification du personnel de sécurité qui devra effectuer une analyse des répercussions avant la mise en œuvre des modifications. Contrôle connexe : SA-10.

Améliorations du contrôle :

(1) L'organisation confie la responsabilité du développement du processus de gestion de la configuration à des employés de l'organisation qui ne participent pas directement au développement du système.

Conseils supplémentaires d'amélioration : En l'absence d'une équipe chargée spécifiquement de la gestion de la configuration, on peut confier à l'intégrateur de système la tâche de développer le processus de gestion.

Références :

Aucune.

4.6 FAMILLE : PLANIFICATION D'URGENCE

CLASSE : OPÉRATIONNELLE

CP-1 POLITIQUE ET PROCÉDURES DE PLANIFICATION D'URGENCE

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique de planification d'urgence formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de planification d'urgence et des contrôles correspondants.

(AA) L'organisation développe un cycle de vérification du programme de planification d'urgence comme base de déclaration régulière au SCT.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de planification d'urgence. La politique et les procédures de planification d'urgence sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique de planification d'urgence peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures de planification d'urgence peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique de planification d'urgence. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

Norme opérationnelle de sécurité - Programme de planification de la continuité des activités (PCA) du SCT [Référence 12].
*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].
Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].

CP-2 PLAN DES MESURES D'URGENCE

Contrôle :

(A) L'organisation développe pour le système d'information un plan de mesures d'urgence qui :

(a) Identifie les fonctions opérationnelles et de mission essentielles et les exigences d'urgence connexes;

(b) Définit les objectifs de reprise, les priorités de restauration et les paramètres;

(c) Identifie les rôles et responsabilités liés aux urgences et les individus assignés à ces fonctions, incluant l'information pour les contacter;

(d) Souligne le besoin de maintenir les fonctions opérationnelles et de mission essentielles en dépit de toute perturbation, compromission ou défaillance du système d'information;

(e) Traite de la restauration complète du système d'information sans détérioration des mesures de sécurité initialement prévues et instaurées; et

(f) Est révisé et approuvé par des agents désignés de l'organisation.

(B) L'organisation distribue des copies du plan des mesures d'urgence à [*Affectation : liste (par nom et (ou) rôle) définie par l'organisation des principaux responsables des mesures d'urgence et des éléments organisationnels*].

(C) L'organisation coordonne les activités de planification d'urgence avec les activités de traitement des incidents.

(D) L'organisation examine le plan des mesures d'urgence du système d'information [*Affectation : fréquence définie par l'organisation*].

(E) L'organisation révise le plan des mesures d'urgence pour tenir compte des changements apportés à l'organisation, au système d'information ou à l'environnement d'exploitation et des problèmes rencontrés lors de la mise en œuvre, de l'exécution ou des tests du plan.

(F) L'organisation communique les modifications du plan des mesures d'urgence à [*Affectation : liste (par nom et (ou) rôle) définie par l'organisation des principaux responsables des mesures d'urgence et des éléments organisationnels*].

Conseils supplémentaires : La planification d'urgence des systèmes d'information fait partie du programme global de l'organisation sur le maintien des activités liées à la mission et (ou) aux opérations. Elle tient compte à la fois, dans les situations de compromission, de la restauration du système et de la mise en œuvre de processus de secours liés à la mission et aux opérations. Les objectifs de reprise du système sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. En plus des événements qui menacent la disponibilité du système, le plan aborde également les autres événements de sécurité susceptibles de réduire l'efficacité de la mission et (ou) des opérations, telles les attaques malveillantes qui compromettent la confidentialité ou l'intégrité du système. Les mesures invoquées par le plan incluent, par exemple, la dégradation progressive, l'arrêt du système, le passage en mode manuel, l'utilisation d'un flux d'information de secours ou le fonctionnement en mode réservé aux situations d'attaque. Contrôles connexes : AC-14, CP-6, CP-7, CP-8, IR-4, PM-8, PM-11.

Améliorations du contrôle :

(1) L'organisation coordonne le développement du plan des mesures d'urgence avec les éléments organisationnels responsables des plans connexes.

Conseils supplémentaires d'amélioration : Exemples de plans connexes : plan de continuité des activités, plan de reprise après sinistre, plan de continuité des opérations, plan des communications en temps de crise, plan de l'infrastructure essentielle, plan d'intervention en cas d'incident cybernétique et plan de mesures d'urgence pour les occupants.

(2) L'organisation planifie la capacité de manière à disposer des ressources nécessaires pour traiter l'information, utiliser les télécommunications et soutenir l'environnement durant les opérations d'urgence.

(3) L'organisation planifie la reprise des fonctions opérationnelles et de mission essentielles dans les [*Affectation : durée définie par l'organisation] pour l'activation du plan des mesures d'urgence]*.

(4) L'organisation planifie la reprise complète des fonctions opérationnelles et de mission dans les [*Affectation : durée définie par l'organisation] pour l'activation du plan des mesures d'urgence*].

(5) L'organisation planifie la continuité des fonctions opérationnelles et de mission essentielles avec peu ou pas de perte au plan de la continuité des activités et maintient cet état jusqu'à la restauration complète du système d'information dans les sites principaux de traitement et (ou) de stockage.

(6) L'organisation prévoit le transfert de toutes les fonctions opérationnelles et de mission essentielles vers des sites principaux de traitement et (ou) de stockage de secours avec peu ou pas de perte au plan de la continuité des activités, et maintient cet état pendant la restauration complète dans ces sites.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].
SCT Norme opérationnelle de sécurité – Programme de planification de la continuité des activités (PCA) [Référence 12].
Norme opérationnelle de sécurité - Niveaux de préparation des installations du gouvernement fédéral du SCT [Référence 13].
Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].

CP-3 FORMATION SUR LES SITUATIONS D'URGENCE

Contrôle :

(A) L'organisation assure la formation du personnel sur ses rôles et responsabilités lors des urgences liées au système d'information et offre des cours de recyclage [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Aucune.

Améliorations du contrôle :

(1) L'organisation intègre des événements simulés à la formation sur les situations d'urgence pour faciliter l'intervention efficace du personnel en situations de crise.

(2) L'organisation utilise des mécanismes automatisés pour créer un environnement de formation plus complet et réaliste.

Références :

Aucune.

CP-4 TESTS ET EXERCICES RELATIFS AU PLAN DES MESURES D'URGENCE

Contrôle :

(A) L'organisation teste et (ou) vérifie l'applicabilité du plan des mesures d'urgence du système d'information [*Affectation : fréquence définie par l'organisation*] en utilisant [*Affectation : tests et (ou) exercices définis par l'organisation*] pour en déterminer l'efficacité et établir la mesure dans laquelle elle est prête à l'exécuter.

(B) L'organisation examine les résultats des tests et des exercices relatifs au plan et entreprend des mesures correctrices.

Conseils supplémentaires : Il existe plusieurs méthodes de test et (ou) de vérification de l'applicabilité du plan des mesures d'urgences pour identifier les faiblesses potentielles (p. ex., liste de vérification, revue de projet et analyse, simulation en parallèle et en état d'arrêt complet). Les tests et (ou) les exercices incluent une détermination des effets des opérations d'urgence conformes au plan sur les activités et les biens de l'organisation (p. ex., réduction de la capacité de la mission) et sur les individus.

Améliorations du contrôle :

(1) L'organisation coordonne les tests et (ou) les exercices relatifs au plan des mesures d'urgence avec les éléments organisationnels responsables des plans connexes.

Conseils supplémentaires d'amélioration : Exemples de plans connexes : plan de continuité des activités, plan de reprise après sinistre, plan de continuité des opérations, plan de reprise des activités, plan d'intervention en cas d'incident et plan d'action d'urgence.

(2) L'organisation teste et (ou) vérifie l'applicabilité du plan des mesures d'urgence dans le site de traitement de secours afin de permettre au personnel de se familiariser avec l'installation et les ressources disponibles et d'évaluer la capacité du site de prendre en charge les opérations d'urgence.

(3) L'organisation utilise des mécanismes automatisés pour tester et (ou) vérifier plus en détail et plus efficacement l'applicabilité du plan des mesures d'urgence en assurant une couverture plus complète des situations d'urgence, en sélectionnant des scénarios et des environnements de test et d'exercice plus réalistes et en soumettant plus efficacement le système et les missions concernées à des contraintes.

(4) L'organisation inclut dans les tests du plan des mesures d'urgence une récupération et une reconstitution complètes du système d'information à un état connu.

Conseils supplémentaires d'amélioration : Contrôles connexes : CP-10, SC-24.

Références :

Aucune.

CP-5 MISE À JOUR DU PLAN DES MESURES D'URGENCE

[Annulé : Intégré au contrôle CP-2].

CP-6 SITES DE STOCKAGE DE SECOURS

Contrôle :

(A) L'organisation établit un site de stockage de secours, incluant les ententes nécessaires pour permettre le stockage et la récupération de l'information sur la sauvegarde des systèmes.

Conseils supplémentaires : Contrôles connexes : CP-2, CP-9, MP-4.

Améliorations du contrôle :

(1) L'organisation identifie un site de stockage de secours distinct du site principal afin de n'être pas assujettie aux mêmes risques.

Conseils supplémentaires d'amélioration : Les situations préoccupantes pour l'organisation sont normalement définies lors d'une évaluation des risques.

(2) L'organisation configure le site de secours de manière à faciliter les opérations de reprise en conformité avec les objectifs de temps et de point de reprise.

(3) L'organisation identifie les problèmes d'accessibilité potentiels du site stockage de secours dans l'éventualité d'une perturbation ou d'un désastre majeurs et énonce des mesures d'atténuation explicites.

Conseils supplémentaires d'amélioration : Les mesures d'atténuation explicites incluent, par exemple, la duplication de l'information de sauvegarde dans un autre site de stockage lorsque l'accès au premier site de secours est entravé, ou, dans l'éventualité d'une interruption de l'accès électronique au site de secours, la planification d'un accès physique pour récupérer l'information de sauvegarde.

Références :

Aucune.

CP-7 SITE DE TRAITEMENT DE SECOURS

Contrôle :

(A) L'organisation établit un site de traitement de secours, incluant les ententes nécessaires pour permettre la reprise des opérations du système d'information pour les fonctions opérationnelles et de mission essentielles dans les [*Affectation : durée conforme aux objectifs de temps de reprise définie par l'organisation*], lorsque les capacités de traitement principales ne sont pas disponibles.

(B) L'organisation s'assure que l'équipement et les fournitures nécessaires à la reprise des opérations sont disponibles dans le site de secours, ou qu'il existe des contrats pour qu'ils soient livrés à temps afin de respecter la durée de la reprise qu'elle a définit.

Conseils supplémentaires : Contrôle connexe : CP-2.

Améliorations du contrôle :

(1) L'organisation identifie un site de traitement de secours distinct du site principal afin de n'être pas assujettie aux mêmes risques.

Conseils supplémentaires d'amélioration : Les situations préoccupantes pour l'organisation sont normalement définies lors d'une évaluation des risques.

(2) L'organisation identifie les problèmes d'accessibilité potentiels du site stockage de secours dans l'éventualité d'une perturbation ou d'un désastre majeurs et énonce des mesures d'atténuation explicites.

(3) L'organisation développe pour le site de traitement de secours des ententes qui prévoient des dispositions de priorité de service en conformité avec les exigences de disponibilité de l'organisation.

(4) L'organisation configure le site de traitement de secours de manière qu'il soit prêt à être utilisé comme site opérationnel pour le traitement des fonctions opérationnelles et de mission essentielles.

(5) L'organisation s'assure que le site de traitement de secours offre des mesures de protection de la sécurité de l'information équivalentes à celles du site principal.

Références :

Aucune.

CP-8 SERVICES DE TÉLÉCOMMUNICATIONS

Contrôle :

(A) L'organisation établit des services de télécommunications de secours, incluant les ententes nécessaires pour permettre, dans les [*Affectation : durée définie par l'organisation*], la reprise des opérations du système d'information liées aux fonctions opérationnelles et de mission essentielles, lorsque les capacités de télécommunications principales ne sont pas disponibles.

Conseils supplémentaires : Contrôle connexe : CP-2.

Améliorations du contrôle :

(1) L'organisation :

(a) Développe des ententes de services de télécommunications de première ligne et de secours qui incluent des dispositions sur la priorité de service, en conformité avec ses exigences de disponibilité; et

(b) Demande l'établissement d'une priorité de service pour tous les services de télécommunications utilisés dans le cadre des activités de protection civile dans l'éventualité où les services de télécommunications de première ligne et (ou) de secours sont assurés par une entreprise de télécommunications.

(2) L'organisation obtient les services de télécommunications de secours en tenant compte du besoin de réduire la probabilité de partage d'un point de défaillance unique avec les services de télécommunications de première ligne.

(3) L'organisation identifie des fournisseurs de services de télécommunications de secours différents des fournisseurs de première ligne afin de n'être pas assujettie aux mêmes risques.

(4) L'organisation exige des fournisseurs de première ligne et de services de secours qu'ils possèdent des plans de mesures d'urgence.

Références :

Aucune.

CP-9 SAUVEGARDE DES SYSTÈMES D'INFORMATION

Contrôle :

(A) L'organisation effectue des sauvegardes des données d'utilisateur contenues dans le système d'information [*Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise*].

(B) L'organisation effectue des sauvegardes des données système contenues dans le système d'information [*Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise*].

(C) L'organisation effectue des sauvegardes de la documentation du système, incluant la documentation sur la sécurité, [*Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise*].

(D) L'organisation protège la confidentialité et l'intégrité de l'information sauvegardée dans le lieu de stockage, en conformité avec la *Norme opérationnelle sur la sécurité matérielle du SCT* [Référence 7].

(AA) L'organisation détermine les périodes de conservation de l'information opérationnelle essentielle et des sauvegardes archivées.

Conseils supplémentaires : L'information système inclut, par exemple, l'information d'état, le système d'exploitation et le logiciel d'application, et les licences. Les signatures numériques et les hachages cryptographiques sont des exemples de mécanismes que les organisations peuvent utiliser pour protéger l'intégrité des sauvegardes de système. Une évaluation des risques permet à l'organisation de décider de la façon d'utiliser le chiffrement pour protéger l'information de sauvegarde. La protection de l'information sur les sauvegardes de système en transit est hors de la portée de ce contrôle. Contrôles connexes : CP-6, MP-4.

Améliorations du contrôle :

(1) L'organisation effectue des tests de l'information de sauvegarde [*Affectation : fréquence définie par l'organisation*] pour vérifier la fiabilité des supports et l'intégrité de l'information.

(2) L'organisation utilise un échantillon de l'information de sauvegarde pour restaurer certaines fonctions du système d'information dans le cadre des tests du plan des mesures d'urgence.

(3) L'organisation conserve des copies de sauvegarde du système d'exploitation et des autres logiciels critiques du système d'information, ainsi que des copies de l'inventaire du système d'information (incluant les composantes matérielles, logicielles et micrologicielles), dans une installation distincte ou un conteneur résistant au feu situé hors de l'emplacement du système de production.

(4) [Annulée : Intégrée au contrôle CP-9].

(5) L'organisation transfère l'information sur la sauvegarde des systèmes d'information dans un site de stockage de secours [*Affectation : durée et taux de transfert définis par l'organisation et conformes aux objectifs de temps et de point de reprise*].

(6) L'organisation effectue la sauvegarde des systèmes en recourant à un système secondaire redondant qui peut être activé sans perte d'information ni perturbation du fonctionnement des systèmes.

Références :

Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7].
*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

CP-10 RÉCUPÉRATION ET RECONSTITUTION DES SYSTÈMES D'INFORMATION

Contrôle :

(A) L'organisation permet la récupération et la reconstitution du système d'information à un état connu après une interruption, une compromission ou une défaillance.

Conseils supplémentaires : La reprise consiste à exécuter activités du plan des mesures d'urgence du système d'information pour récupérer les fonctions opérationnelles et de mission essentielles. Le reconstitution suit la récupération et inclut les activités de retour du système à son état fonctionnel initial (avant l'activation du plan des mesures d'urgence). Les procédures de récupération et de reconstitution sont basées sur les priorités organisationnelles, le temps et le point de reprise préétablis, les objectifs de la reconstitution et les paramètres appropriés. La reconstitution inclut la désactivation de toute capacité de système intérimaire potentiellement activée durant les opérations de récupération. Elle inclut également une évaluation de la capacité du système entièrement restauré, une réautorisation potentielle du système et les activités requises pour préparer le système à affronter toute autre perturbation, compromission ou défaillance. Les capacités de récupération et de reconstitution utilisées par l'organisation peuvent être une combinaison de mécanismes automatisés et de procédures manuelles. Contrôles connexes : CA-2, CA-6, CA-7, CP-4, SC-24.

Améliorations du contrôle :

(1) [Annulée : Intégrée au contrôle CP-4].

(2) Le système applique un processus de récupération des transactions pour les systèmes de traitement transactionnel.

Conseils supplémentaires d'amélioration : Les systèmes de gestion de base de données et les systèmes de traitement transactionnel sont des exemples de systèmes d'information axés sur les transactions. Les mécanismes d'annulation et de journalisation de transactions sont des exemples de mécanismes qui permettent la récupération des transactions.

(3) L'organisation prévoit des contrôles de sécurité compensatoires pour [*Affectation : circonstances définies par l'organisation qui peuvent nuire à la récupération et à la reconstitution à un état connu*].

(4) L'organisation permet de rétablir l'image des composantes de système d'information dans les [*Affectation : durées de restauration définies par l'organisation*] en utilisant des images disque (dont la configuration est contrôlée et l'intégrité, protégée) représentant les composantes dans un état protégé et opérationnel.

(5) L'organisation offre [*Sélection : temps réel; temps presque réel*] [*Affectation : capacité de reprise définie par l'organisation*].

Conseils supplémentaires d'amélioration : Les exemples de capacité de reprise incluent la copie du miroitage des opérations du système d'information dans un site de traitement de secours ou le miroitage périodique des données à intervalles réguliers durant une période définie par la durée de reprise de l'organisation.

(6) L'organisation protège le matériel, le micrologiciel et le logiciel de sauvegarde et de restauration.

Conseils supplémentaires d'amélioration : La protection du matériel, du micrologiciel et du logiciel de sauvegarde et de restauration inclut des mesures à la fois physiques et techniques. Les tableaux de routeur, les compilateurs et autres systèmes logiciels de sécurité sont des exemples de logiciel de sauvegarde et de restauration.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

4.7 FAMILLE : IDENTIFICATION ET AUTHENTIFICATION

CLASSE : TECHNIQUE

IA-1 POLITIQUE ET PROCÉDURES D'IDENTIFICATION ET D'AUTHENTIFICATION

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique d'identification et d'authentification formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique d'identification et d'authentification et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles d'identification et d'authentification. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique d'identification et d'authentification peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures d'identification et d'authentification peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique d'identification et d'authentification. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

IA-2 IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)

Contrôle :

(A) Le système d'information identifie de façon unique et authentifie les utilisateurs organisationnels (ou les processus exécutés en leur nom).

Conseils supplémentaires : Les utilisateurs organisationnels incluent les employés ou les personnes dont l'organisation juge le statut équivalent à celui d'un employé (p. ex., entrepreneurs, chercheurs invités, représentants de nations alliées). Les utilisateurs sont identifiés de façon unique et authentifiés pour tous les accès autres que ceux explicitement identifiés et documentés par l'organisation dans le contrôle AC-14. On devra peut-être envisager d'identifier chaque individu inclus dans les comptes de groupe (p. ex., comptes privilégiés partagés) aux fins de comptabilisation détaillée de l'activité. Pour authentifier les identités des employés, on utilise des mots de passe, des jetons, des données biométriques, ou, dans le cas d'une authentification multifactorielle, une combinaison de ces paramètres. L'accès aux systèmes d'information

organisationnels est soit un accès local, soit un accès réseau. Un accès local est tout accès par un utilisateur (ou par un processus exécuté en son nom) effectué par une connexion directe, sans recours à un réseau. Un accès réseau est tout accès par un utilisateur (ou par un processus exécuté en son nom) effectué par une connexion réseau. L'accès à distance est un type d'accès réseau qui requiert une communication par un réseau externe (p. ex., Internet). Les réseaux internes incluent les réseaux locaux, les réseaux étendus et les réseaux privés virtuels (RPV) contrôlés par l'organisation. Le RPV est considéré un réseau interne si l'organisation établit la connexion entre des points d'extrémité qu'elle contrôle de manière à ne pas utiliser de réseaux externes pour protéger la confidentialité et l'intégrité de l'information transmise. Les exigences d'identification et d'authentification pour l'accès par des personnes autres que les utilisateurs organisationnels sont décrits dans le contrôle IA-8.

En plus de permettre l'identification et l'authentification des utilisateurs au niveau du système d'information (c.-à-d., au moment de la connexion), les mécanismes d'identification et d'authentification sont utilisés au niveau de l'application, le cas échéant, pour accroître la sécurité de l'information. Contrôles connexes : AC-14, AC-17, AC-18, IA-4, IA-5.

Améliorations du contrôle :

(1) Le système utilise l'authentification multifactorielle pour l'accès réseau aux comptes privilégiés.

(2) Le système utilise l'authentification multifactorielle pour l'accès réseau aux comptes non privilégiés.

(3) Le système utilise l'authentification multifactorielle pour l'accès local aux comptes privilégiés.

(4) Le système utilise l'authentification multifactorielle pour l'accès local aux comptes non privilégiés.

(5) L'organisation :

(a) Permet l'utilisation d'authentifiants de groupe seulement s'ils sont utilisés de pair avec un authentifiant individuel ou unique; et

(b) Exige des utilisateurs qu'ils soient authentifiés par un authentifiant individuel avant d'utiliser un authentifiant de groupe.

(6) Le système utilise l'authentification multifactorielle pour l'accès réseau aux comptes privilégiés; un des facteurs doit être fourni par un dispositif distinct du système d'information auquel l'utilisateur accède.

(7) Le système utilise l'authentification multifactorielle pour l'accès réseau aux comptes non privilégiés; un des facteurs doit être fourni par un dispositif distinct du système d'information auquel l'utilisateur accède.

(8) Le système utilise [*Affectation : mécanismes d'authentification résistants aux réinsertions définis par l'organisation*] pour l'accès réseau aux comptes privilégiés.

Conseils supplémentaires d'amélioration : Un processus d'authentification résiste aux attaques par réinsertion lorsqu'il est impossible en pratique de réussir une authentification en enregistrant puis en réinsérant un message d'authentification antérieur. Les techniques pour contourner ce problème incluent les protocoles qui utilisent des valeurs ponctuelles (nonces) ou des défis (p. ex., TLS) et les authentifiants défi-réponse synchrones à usage unique.

(9) Le système utilise [*Affectation : mécanismes d'authentification résistants aux réinsertions définis par l'organisation*] pour l'accès réseau aux comptes non privilégiés.

Conseils supplémentaires d'amélioration : Un processus d'authentification résiste aux attaques par réinsertion lorsqu'il est impossible en pratique de réussir une authentification en enregistrant puis en réinsérant un message d'authentification antérieur. Les techniques pour contourner ce problème incluent les protocoles qui utilisent des valeurs ponctuelles (nonces) ou des défis (p. ex., TLS) et les authentifiants défi-réponse synchrones à usage unique.

(100) Le système d'information utilise l'authentification multifactorielle pour l'accès à distance aux comptes privilégiés.

Conseils supplémentaires d'amélioration : La connexion à distance au réseau s'entend de toute connexion effectuée au moyen d'un dispositif qui communique à travers un réseau externe non fiabilisé (p. ex. Internet). Contrôles connexes : AC-17, AC-18

Références :

Guide sur l'authentification des utilisateurs pour les systèmes TI (ITSG-31) du CSTC [Référence 19].

Conseils sur l'utilisation du protocole TLS (Transport Layer Security) au sein du gouvernement du Canada (ITSB-60) du CSTC [Référence 35].

IA-3 IDENTIFICATION ET AUTHENTIFICATION DES DISPOSITIFS

Contrôle :

(A) Le système d'information identifie de façon unique et authentifie [*Affectation : liste définie de dispositifs spécifiques et (ou) de types of dispositif*] avant l'établissement d'une connexion.

Conseils supplémentaires : Les dispositifs qui doivent être identifiés de façon unique et authentifiés peuvent être définis par type et modèle spécifique, ou une combinaison des deux, selon ce que l'organisation juge approprié. Le système d'information utilise normalement aux fins d'identification soit de l'information partagée connue (p. ex., adresses MAC (contrôle d'accès aux supports) ou TCP/IP (Transmission Control Protocol/Internet Protocol)) ou une solution d'authentification organisationnelle (p. ex., IEEE 802.1x et EAP, serveur Radius avec authentification EAP-TLS, Kerberos) pour identifier et authentifier les dispositifs des réseaux locaux et (ou) étendus. La force requise du mécanisme d'authentification de dispositif est déterminée par les catégories de sécurité du système d'information.

Améliorations du contrôle :

(1) Le système authentifie les dispositifs avant l'établissement des connexions réseau à distance et sans fil en utilisant une authentification bidirectionnelle cryptographique entre dispositifs.

Conseils supplémentaires d'amélioration : Une connexion réseau à distance est toute connexion à un dispositif qui communique par un réseau externe (p. ex., Internet). Contrôles connexes : AC-17, AC-18.

(2) Le système authentifie les dispositifs avant l'établissement des connexions réseau en utilisant une authentification bidirectionnelle cryptographique entre dispositifs.

(3) L'organisation, pour l'attribution dynamique des adresses, normalise l'information de bail et l'heure DHCP attribuées aux dispositifs et vérifie l'information de bail lors de son attribution à un dispositif.

Conseils supplémentaires d'amélioration : Pour ce qui concerne l'attribution dynamique des adresses aux dispositifs, les clients DHCP obtiennent normalement des serveurs DHCP les *baux* pour les adresses IP.

Références :

Aucune.

IA-4 GESTION DES IDENTIFICATEURS

Contrôle :

(A) L'organisation gère les identificateurs d'utilisateur et de dispositif sous l'autorité d'un agent désigné de l'organisation chargé de leur attribution.

(B) L'organisation gère les identificateurs d'utilisateur et de dispositif en sélectionnant un identificateur d'utilisateur ou de dispositif unique.

(C) L'organisation gère les identificateurs d'utilisateur et de dispositif en attribuant l'identificateur à l'utilisateur ou au dispositif concerné.

(D) L'organisation gère les identificateurs d'utilisateur et de dispositif en empêchant leur réutilisation pendant [*Affectation : durée définie par l'organisation*].

(E) L'organisation gère les identificateurs d'utilisateur et de dispositif en désactivant l'identificateur d'utilisateur après [*Affectation : durée d'inactivité définie par l'organisation*].

Conseils supplémentaires : Les identificateurs de dispositif courants incluent les adresses MAC ou IP, ou les identificateurs à jeton unique. La gestion des identificateurs d'utilisateur ne s'applique pas aux comptes partagés (p. ex., comptes d'invité et anonymes). Normalement, un identificateur d'utilisateur est le nom d'un compte de système associé à un individu. Dans ce contexte, la gestion des identificateurs relève dans une large mesure des activités de gestion de comptes du contrôle AC-2. Le contrôle IA-4 traite également des identificateurs d'utilisateur non nécessairement associés à un compte de système (p. ex., un identificateur utilisé dans une base de données de contrôle de la sécurité physique consultée par un système de lecture de badges aux fins d'accès au système). Contrôles connexes : AC-2, IA-2.

Améliorations du contrôle :

(1) L'organisation interdit l'utilisation des identificateurs de compte de système comme identificateurs publics des comptes de courrier électronique d'utilisateur (c.-à-d., la partie identificateur d'utilisateur de l'adresse électronique).

Conseils supplémentaires d'amélioration : L'organisation applique cette amélioration dans la mesure où le système d'information le permet.

(2) L'organisation exige que la demande d'attribution d'un Id. d'utilisateur et d'un mot de passe inclue l'autorisation d'un superviseur et soit formulée en personne devant une autorité d'enregistrement désignée.

(3) L'organisation exige plusieurs formes de certification d'identification individuelle, telle la présentation à l'autorité d'enregistrement d'un document probant ou d'une combinaison de documents et de données biométriques.

(4) L'organisation gère les identificateurs d'utilisateur en identifiant de façon unique l'utilisateur comme [*Affectation : caractéristique définie par l'organisation identifiant le statut de l'utilisateur*].

Conseils supplémentaires d'amélioration : Les caractéristiques identifiant le statut de l'utilisateur incluent, par exemple, le statut d'entrepreneur et de ressortissant étranger.

(5) Le système gère de manière dynamique les identificateurs, les attributs et les autorisations d'accès correspondantes.

Conseils supplémentaires d'amélioration : Contrairement aux approches conventionnelles d'identification et d'authentification qui utilisent l'information statique de compte de système pour les utilisateurs préenregistrés, plusieurs des architectures axées sur les services recourent à l'identification en temps réel dans le cas des entités jusque là inconnues. Il est essentiel de pouvoir compter sur des relations de confiance préétablies et des mécanismes possédant les autorités appropriées pour valider les identités et leurs justificatifs.

Références :

Aucune.

IA-5 GESTION DES AUTHENTIFIANTS

Contrôle :

(A) L'organisation gère les authentifiants d'utilisateur et de dispositif en vérifiant, au moment de la distribution initiale des authentifiants, l'identité de l'utilisateur et (ou) du dispositif authentifié.

(B) L'organisation gère les authentifiants d'utilisateur et de dispositif en établissant le contenu initial des authentifiants définis par l'organisation.

(C) L'organisation gère les authentifiants d'utilisateur et de dispositif en s'assurant que le mécanisme d'authentification possède la force appropriée à l'utilisation prévue.

(D) L'organisation gère les authentifiants d'utilisateur et de dispositif en établissant et appliquant les procédures administratives nécessaires (distribution initiale des authentifiants, authentifiants perdus, compromis ou endommagés et révocation des authentifiants).

(E) L'organisation gère les authentifiants d'utilisateur et de dispositif en modifiant le contenu par défaut des authentifiants au moment de l'installation du système.

(F) L'organisation gère les authentifiants d'utilisateur et de dispositif en établissant les restrictions minimales et maximales de durée et les conditions de réutilisation des authentifiants (le cas échéant).

(G) L'organisation gère les authentifiants d'utilisateur et de dispositif en modifiant et (ou) actualisant les authentifiants [*Affectation : durée définie par l'organisation par type d'authentifiant*].

(H) L'organisation gère les authentifiants d'utilisateur et de dispositif en protégeant le contenu de l'authentifiant contre toute divulgation et modification non autorisées.

(I) L'organisation gère les authentifiants d'utilisateur et de dispositif en exigeant des utilisateurs et des dispositifs qu'ils appliquent des mesures spécifiques de protection des authentifiants.

Conseils supplémentaires : Les authentifiants d'utilisateur incluent, par exemple, les mots de passe, les jetons, les données biométriques, les certificats d'ICP et les cartes clés. Le contenu initial de l'authentifiant est le contenu réel (p. ex., le mot de passe initial) et non les exigences relatives au contenu (p. ex., la longueur minimale du mot de passe). Plusieurs composantes de système d'information sont livrées avec les justificatifs d'authentification par défaut du fabricant pour permettre l'installation et la configuration initiales du produit. Ces justificatifs sont souvent bien connus et facilement décryptables et posent un risque sérieux à la sécurité; ils doivent donc être changés au moment de l'installation. Les exigences de protection des authentifiants d'utilisateur peuvent être appliquées par les contrôles PL-4 ou PS-6 et celles des authentifiants stockés dans le système d'information, par les contrôles AC-3, AC-6 et SC-28 (p. ex., mots de passe stockés sous forme hachurée ou chiffrée, fichiers contenant des mots de passe hachurés ou chiffrés accessibles seulement avec des privilèges de super utilisateur). Le système assure une gestion des authentifiants d'utilisateur basée sur les paramètres et les restrictions définis par l'organisation pour différentes caractéristiques d'authentification, entre autres : longueur minimale et composition des mots de passe, fenêtre de validation des jetons à utilisation unique et nombre de rejets permis durant le stade de vérification d'une authentification biométrique. Les mesures de protection des authentifiants d'utilisateur incluent, par exemple, la protection de la possession des authentifiants individuels, l'interdiction de prêter ou de partager les authentifiants avec d'autres employés et le signalement dans les plus brefs délais des authentifiants perdus ou compromis. La gestion des authentifiants inclut l'émission puis la révocation, lorsqu'ils ne sont plus requis, des authentifiants utilisés pour un accès temporaire (p. ex., pour la maintenance à distance). Les authentifiants de dispositif incluent, par exemple, les certificats et les mots de passe. Contrôles connexes : AC-2, IA-2, PL-4, PS-6.

Améliorations du contrôle :

(1) Authentification axée sur les mots de passe – Le système :

(a) Applique un mot de passe de complexité minimale [*Affectation : exigences définies par l'organisation concernant la sensibilité à la casse, le nombre de caractères, la combinaison minuscules-majuscules, les lettres minuscules, les chiffres et les caractères spéciaux, incluant les exigences minimales pour chaque type*];

(b) Utilise au minimum [*Affectation : nombre de caractères modifiables défini par l'organisation*] lors de la création de nouveaux mots de passe;

(c) Chiffre les mots de passe stockés et en transit;

(d) Applique les restrictions minimales et maximales de durée des mots de passe [*Affectation : nombre défini par l'organisation pour la durée minimale ou maximale*]; et

(e) Interdit la réutilisation des mots de passe pendant [*Affectation : nombre défini par l'organisation*] générations.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle concerne principalement les environnements qui utilisent les mots de passe comme facteur unique d'authentification des utilisateurs, ou qui utilisent des mots de passe combinés à un ou plusieurs authentifiants supplémentaires. Elle ne s'applique *pas* de manière générale aux situations où les mots de passe servent à déverrouiller des authentifiants matériels. L'application de ces mécanismes de mot de passe peut ne pas satisfaire aux exigences de l'amélioration.

(2) Authentification axée sur l'ICP – Le système :

(a) Valide les certificats en créant une voie de certification, incluant de l'information d'état, vers un ancrage de confiance autorisé;

(b) Applique la procédure d'accès autorisé à la clé privée correspondante; et

(c) Associe l'identité authentifiée au compte de l'utilisateur.

Conseils supplémentaires d'amélioration : L'information d'état pour les voies de certification inclut, par exemple, les listes de certificats révoqués ou les réponses en ligne d'un protocole de statut de certificat.

(3) L'organisation exige que la procédure de demande de [*Affectation : types d'authentifiant et (ou) authentifiants spécifiques définis par l'organisation*] soit effectuée en personne auprès d'une autorité d'enregistrement désignée avec l'autorisation d'un agent désigné de l'organisation (p. ex., un superviseur).

(4) L'organisation utilise des outils automatisés pour déterminer si les authentifiants sont suffisamment forts pour résister aux attaques conçues pour les décrypter ou les compromettre.

(5) L'organisation exige des fournisseurs et (ou) des fabricants des composantes de système d'information qu'ils fournissent des authentifiants uniques ou qu'ils changent les authentifiants par défaut avant la livraison.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle étend l'exigence selon laquelle les organisations doivent modifier les authentifiants par défaut au moment de l'installation du système d'information; à cette fin, elles doivent exiger des fournisseurs et (ou) fabricants des composantes qu'ils fournissent des authentifiants uniques ou modifient les authentifiants par défaut des composantes avant leur livraison. Les authentifiants uniques sont assignés par les fournisseurs et (ou) les fabricants aux composantes individuelles (c.-à-d., produits de technologie de l'information livrés) possédant des numéros de série distincts. Cette exigence est incluse dans les documents d'acquisition préparés par l'organisation lors de l'achat des systèmes d'information et (ou) des composantes.

(6) L'organisation protège les authentifiants au niveau de sécurité qui correspond à la sensibilité et à la criticité de l'information et du système d'information concernés.

(7) L'organisation s'assure qu'aucun authentifiant statique chiffré n'est intégré à des applications ou à des scripts d'accès, ni activé par des touches de fonctions.

Conseils supplémentaires d'amélioration : Les organisations doivent prendre soin de déterminer si les authentifiants intégrés ou stockés sont chiffrés ou non. Si un authentifiant est utilisé tel qu'il est stocké, il est considéré non chiffré, peu importe que sa représentation soit une version chiffrée d'une valeur quelconque (p. ex., un mot de passe).

(8) L'organisation prend [*Affectation : mesures définies par l'organisation*] pour gérer le risque de compromission que posent les utilisateurs qui possèdent des comptes dans plusieurs systèmes d'information.

Conseils supplémentaires d'amélioration : Lorsqu'un utilisateur possède des comptes dans plusieurs systèmes, si un compte est compromis et que l'utilisateur se sert du même identificateur et du même authentifiant pour d'autres systèmes, il peut arriver que d'autres comptes soient également compromis. Les alternatives pour éviter ce problème incluent, sans s'y limiter, les suivantes : (i) utiliser le même identificateur d'utilisateur mais des authentifiants différents pour tous les systèmes; (ii) utiliser des identificateurs d'utilisateur et des authentifiants différents pour chaque système; (iii) utiliser une forme quelconque de mécanisme unique de connexion; ou (iv) utiliser une forme quelconque de mots de passe à usage unique pour tous les systèmes.

Références :

Guide sur l'authentification des utilisateurs pour les systèmes TI (ITSG-31) du CSTC [Référence 19].

IA-6 OCCULTATION DES AUTHENTIFIANTS

Contrôle :

(A) Le système d'information occulte les rétroactions d'information durant le processus d'authentification afin de protéger l'information contre de possibles exploitations et (ou) utilisations par des personnes non autorisées.

Conseils supplémentaires : Les rétroactions du système d'information ne fournissent aucune donnée qui permettrait à un utilisateur non autorisé de compromettre le mécanisme d'authentification. L'affichage d'astérisques lorsqu'un utilisateur tape son mot de passe est un exemple d'occultation de rétroaction.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

IA-7 AUTHENTIFICATION DES MODULES CRYPTOGRAPHIQUES

Contrôle :

(A) Le système d'information utilise des mécanismes d'authentification basés sur un module cryptographique qui satisfait aux exigences des normes du CSTC en matière d'authentification.

Conseils supplémentaires : Aucune.

Améliorations du contrôle :

Aucune.

Références :

Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés (ITSA-11D) du CSTC [Référence 9].
Guide sur l'authentification des utilisateurs pour les systèmes TI (ITSG-31) du CSTC [Référence 19].
Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B (ITSB-40) du CSTC [Référence 29].

IA-8 IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS NON ORGANISATIONNELS)

Contrôle :

(A) Le système d'information identifie de façon unique et authentifie les utilisateurs non organisationnels (ou les processus exécutés en leur nom).

Conseils supplémentaires : Les utilisateurs non organisationnels incluent tous les utilisateurs autres que les utilisateurs organisationnels explicitement mentionnés dans le contrôle IA-2. Les utilisateurs sont identifiés de façon unique et authentifiés pour tous les types d'accès autres que ceux explicitement identifiés et documentés par l'organisation conformément aux directives du contrôle AC-14. On peut exiger l'authentification des utilisateurs non organisationnels qui accèdent aux systèmes d'information du GC afin de protéger l'information du gouvernement et l'information assujettie aux lois sur la protection des renseignements personnels (sauf les exceptions prévues pour les systèmes liés à la sécurité nationale). On doit donc effectuer une évaluation des risques pour déterminer les besoins d'authentification de l'organisation. L'extensibilité, l'aspect pratique et la sécurité sont pris en compte simultanément pour assurer un juste équilibre entre le besoin d'accéder facilement à l'information et aux systèmes d'information du GC et le besoin de protéger les activités et les biens de l'organisation, les individus et les autres organisations et d'atténuer adéquatement les risques qu'ils encourent. Les exigences d'identification et d'authentification pour les utilisateurs organisationnels qui désirent accéder aux systèmes d'information sont décrits dans le contrôle IA-2. Contrôles connexes : AC-14, AC-17, AC-18, MA-4.

Améliorations du contrôle :

Aucune.

Références :

Guide sur l'authentification des utilisateurs pour les systèmes TI (ITSG-31) du CSTC [Référence 19].

4.8 FAMILLE : INTERVENTION EN CAS D'INCIDENT

CLASSE : OPÉRATIONNELLE

IR-1 POLITIQUE ET PROCÉDURES D'INTERVENTION EN CAS D'INCIDENT

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique d'intervention en cas d'incident formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique d'intervention en cas d'incident et des contrôles correspondants.

(AA) La politique et les procédures d'intervention en cas d'incident de l'organisation facilite l'intégration de niveaux relevés de préparation durant les urgences et les situations de menace des TI élevées, en conformité avec la *Norme opérationnelle de sécurité - Niveaux de préparation des installations du gouvernement fédéral du SCT* [Référence 13] et la *Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8]

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de la politique d'intervention en cas d'incident. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. La politique et les procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique d'intervention peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures d'intervention peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique d'intervention en cas d'incident. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].
Norme opérationnelle de sécurité - Niveaux de préparation des installations du gouvernement fédéral du SCT [Référence 13].
Norme Sécurité relative à l'organisation et l'administration du SCT [Référence 14].
Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].

IR-2 FORMATION SUR LES INTERVENTIONS EN CAS D'INCIDENT

Contrôle :

(A) L'organisation assure la formation du personnel concernant ses rôles et responsabilités relativement aux interventions en cas d'incident liées au système d'information.

(B) L'organisation offre des cours de recyclage [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : La formation sur les interventions en cas d'incident inclut la formation concernant l'identification et la déclaration des activités suspectes de sources à la fois externes et internes. Contrôle connexe : AT-3.

Améliorations du contrôle :

(1) L'organisation intègre des événements simulés à la formation sur les interventions en cas d'incident pour permettre une intervention efficace du personnel en situations de crise.

(2) L'organisation utilise des mécanismes automatisés pour créer un environnement de formation complet plus réaliste.

Références :

Aucune.

IR-3 TESTS ET EXERCICES RELATIFS AUX INTERVENTIONS EN CAS D'INCIDENT

Contrôle :

(A) L'organisation teste et (ou) vérifie la capacité d'intervention en cas d'incidents liés au système d'information [*Affectation : fréquence définie par l'organisation*] en utilisant [*Affectation : tests et (ou) exercices définis par l'organisation*] pour déterminer l'efficacité des interventions et documenter les résultats.

Conseils supplémentaires : Aucune.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour tester et (ou) vérifier plus en détail et plus efficacement la capacité d'intervention en cas d'incident.

Conseils supplémentaires d'amélioration : Les mécanismes automatisés peuvent permettre de tester et (ou) vérifier plus en détail et plus efficacement la capacité d'intervention en assurant une couverture plus complète des situations d'intervention, en sélectionnant des scénarios et des environnements de test et d'exercice plus réalistes et en soumettant plus efficacement la capacité d'intervention à des contraintes. Contrôle connexe : AT-2.

Références :

Aucune.

IR-4 TRAITEMENT DES INCIDENTS

Contrôle :

(A) L'organisation met de l'avant une capacité de traitement des incidents de sécurité qui inclut des activités de préparation, de détection et d'analyse, de confinement, d'éradication et de reprise.

(B) L'organisation coordonne les activités de traitement des incidents avec les activités de planification d'urgence.

(C) L'organisation intègre les leçons apprises au cours des activités de traitement aux procédures d'intervention, à la formation et aux tests et exercices, et applique les résultats obtenus comme il se doit.

Conseils supplémentaires : L'information sur les incidents peut provenir d'une variété de sources incluant, sans s'y limiter, la surveillance des vérifications, des réseaux et de l'accès physique, et les rapports d'utilisateur et (ou) d'administrateur. Contrôles connexes : AU-6, CP-2, IR-2, IR-3, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour soutenir le processus de traitement des incidents.

Conseils supplémentaires d'amélioration : Un système de gestion des incidents en ligne est un exemple de mécanisme automatisé.

(2) L'organisation intègre la reconfiguration dynamique du système d'information à sa capacité d'intervention en cas d'incident.

Conseils supplémentaires d'amélioration : La reconfiguration dynamique inclut, par exemple, les modifications apportées aux règles du routeur, les listes de contrôle d'accès, les paramètres de système de détection et (ou) de prévention d'intrusions, et les règles de filtrage des pare-feu et passerelles.

(3) L'organisation identifie les classes d'incident et définit les mesures d'intervention appropriées pour permettre la continuité de ses missions et fonctions opérationnelles.

Conseils supplémentaires d'amélioration : Les classes d'incident incluent, par exemple, les défectuosités dues aux erreurs ou aux omissions liées à la conception et (ou) à la mise en œuvre, et les attaques malveillantes ciblées et non ciblées. Les mesures d'intervention appropriées incluent, par exemple, la dégradation progressive, l'arrêt du système, le passage au mode manuel ou le recours à une technologie de secours qui permet de faire fonctionner le système différemment, l'utilisation de mesures trompeuses (p. ex., faux flux de données, faux paramètres d'état), l'utilisation d'un flux d'information différent, ou le fonctionnement en mode réservé uniquement aux situations d'attaque.

(4) L'organisation établit une corrélation entre l'information sur les incidents et les interventions individuelles pour obtenir une perspective organisationnelle de la sensibilisation et des interventions en matière d'incident.

(5) L'organisation utilise une capacité configurable qui permet de désactiver automatiquement le système dans l'éventualité de la détection de l'une ou l'autre des violations de sécurité suivantes : [*Affectation : liste des violations de sécurité définie par l'organisation*].

Références :

Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].

IR-5 SURVEILLANCE DES INCIDENTS

Contrôle :

(A) L'organisation piste et documente les incidents de sécurité liés au système d'information.

Conseils supplémentaires : La documentation des incidents de sécurité liés au système d'information inclut, par exemple, la tenue à jour de dossiers sur chaque incident, le statut de l'incident et autres renseignements pertinents pour l'expertise judiciaire, et l'évaluation des détails, des tendances et du traitement des incidents. L'information sur les incidents peut provenir d'une variété de sources incluant, par exemple, les rapports d'incident, les équipes d'intervention, la surveillance des vérifications, des réseaux et de l'accès physique, et les rapports de l'utilisateur et (ou) de l'administrateur.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour faciliter le pistage des incidents de sécurité et la collecte et l'analyse de l'information sur les incidents.

Conseils supplémentaires d'amélioration : Les mécanismes automatisés pour pister les incidents de sécurité et collecter et analyser l'information pertinente incluent, par exemple, la surveillance des centres informatiques d'intervention ou autres bases de données électroniques sur les incidents. Contrôles connexes : AU-6, AU-7, SI-4.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

IR-6 SIGNALEMENT DES INCIDENTS

Contrôle :

(A) L'organisation exige du personnel qu'il signale les incidents de sécurité suspects aux responsables organisationnels des interventions dans les [*Affectation : période définie par l'organisation*].

(B) L'organisation communique l'information sur les incidents de sécurité aux autorités désignées.

Conseils supplémentaires : Le but de ce contrôle est de tenir compte à la fois des exigences spécifiques de l'organisation en matière de signalement des incidents et des exigences formelles de signalement des organismes fédéraux et des organisations qui relèvent de leur autorité. Les types d'incident signalés, le contenu et l'échéancier des rapports et la liste des autorités de déclaration désignées doivent être conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Contrôles connexes : IR-4, IR-5.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour faciliter le signalement des incidents de sécurité.

(2) L'organisation communique aux agents concernés de l'organisation les faiblesses, lacunes et (ou) vulnérabilités du système associées aux incidents signalés.

Références :

Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].

IR-7 ASSISTANCE POUR LES INTERVENTIONS EN CAS D'INCIDENT

Contrôle :

(A) L'organisation fournit les ressources nécessaires au soutien des interventions en cas d'incident, élément essentiel de la capacité d'intervention de l'organisation; ces ressources fournissent des conseils et de l'aide aux utilisateurs du système d'information pour ce qui touche le traitement et le signalement des incidents de sécurité.

Conseils supplémentaires : Les ressources possibles de soutien aux interventions dans une organisation incluent un service de dépannage ou un groupe d'aide, ainsi que l'accès à des services d'expertise judiciaire, le cas échéant. Contrôles connexes : IR-4, IR-6.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour accroître la disponibilité de l'information et du soutien relativement aux incidents de sécurité.

Conseils supplémentaires d'amélioration : Les mécanismes automatisés peuvent offrir aux utilisateurs une capacité d'aide réactive et (ou) proactive lors des interventions. Par exemple, pour accroître leurs connaissances des capacités et des ressources de soutien actuellement offertes, les utilisateurs peuvent accéder à un site Web pour chercher des solutions ou, inversement, une solution particulière offerte sur un site peut leur permettre d'obtenir (par diffusion générale ou ciblée) l'information recherchée.

(2) L'organisation :

(a) Établit une relation de coopération directe entre sa capacité d'intervention et la capacité de protection des systèmes d'information de fournisseurs externes; et

(b) Communique l'identité des membres de son équipe d'intervention aux fournisseurs externes.

Conseils supplémentaires d'amélioration : Les fournisseurs externes aident à la surveillance, l'analyse et la détection des activités illicites dans les systèmes et les réseaux de l'organisation et interviennent, le cas échéant.

Références :

Aucune.

IR-8 PLAN D'INTERVENTION EN CAS D'INCIDENT

Contrôle :

(A) L'organisation développe un plan d'intervention en cas d'incident qui :

(a) Permet à l'organisation de pouvoir compter sur une feuille de route pour la mise en œuvre de sa capacité d'intervention;

(b) Décrit la structure et l'organisation de la capacité d'intervention;

(c) Propose une approche de haut niveau de la façon dont la capacité d'intervention est intégrée à l'ensemble de l'organisation;

(d) Répond à ses exigences spécifiques concernant sa mission, sa taille, sa structure et ses fonctions;

(e) Définit les incidents qui doivent être signalés;

(f) Définit les paramètres de mesure de sa capacité d'intervention;

(g) Définit les ressources et le soutien de la direction nécessaires au maintien et à l'évolution de la capacité d'intervention; et

(h) Est révisé et approuvé par des agents désignés de l'organisation.

(B) L'organisation distribue des copies du plan à [*Affectation : liste définie par l'organisation des employés (par nom et (ou) rôle) chargés des interventions et des éléments organisationnels*].

(C) L'organisation examine le plan [*Affectation : fréquence définie par l'organisation*].

(D) L'organisation révise le plan pour tenir compte des changements dont elle a fait l'objet et (ou) de ceux apportés au système, ou des problèmes relevés au cours de la mise en œuvre, de l'exécution et des tests du plan.

(E) L'organisation communique les changements apportés au plan à [*Affectation : liste définie par l'organisation des employés (par nom et (ou) rôle) chargés des interventions et des éléments organisationnels*].

Conseils supplémentaires : Il est important pour les organisations d'adopter une approche formelle, ciblée et coordonnée d'intervention. La mission, les stratégies et les objectifs de l'organisation à cet égard aident à déterminer la structure de sa capacité d'intervention.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

4.9 FAMILLE : MAINTENANCE

CLASSE : OPÉRATIONNELLE

MA-1 POLITIQUE ET PROCÉDURES DE MAINTENANCE DES SYSTÈMES

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique de maintenance des systèmes d'information formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de maintenance des systèmes d'information et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de maintenance des systèmes. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique de maintenance des systèmes d'information peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures de maintenance peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique de maintenance des systèmes. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

MA-2 MAINTENANCE CONTRÔLÉE

Contrôle :

(A) L'organisation planifie, exécute, documente et examine les dossiers de maintenance et de réparation des composantes de système en conformité avec les spécifications du fabricant ou du fournisseur et (ou) ses propres exigences.

(B) L'organisation contrôle toutes les activités de maintenance, qu'elles soient effectuées sur place ou à distance et que l'équipement soit réparé sur les lieux ou à l'extérieur.

(C) L'organisation exige qu'un agent désigné approuve explicitement le retrait du système, ou des composantes, de ses installations aux fins de maintenance ou de réparation à l'extérieur des locaux.

(D) L'organisation nettoie l'équipement afin de supprimer toutes les données des supports avant de l'expédier à l'extérieur aux fins de maintenance ou de réparation.

(E) L'organisation vérifie tous les contrôles de sécurité potentiellement concernés pour s'assurer qu'ils continuent de fonctionner adéquatement après les activités de maintenance ou de réparation.

Conseils supplémentaires : Le contrôle vise à s'assurer du respect des exigences du programme de maintenance des systèmes d'information de l'organisation en matière de sécurité de l'information. Contrôles connexes : MP-6, SI-2.

Améliorations du contrôle :

(1) L'organisation tient à jour les dossiers de maintenance du système, qui incluent les éléments suivants :

- (a) Date et heure de la maintenance;
- (b) Nom de la personne qui effectue la maintenance;
- (c) Nom de l'escorte, le cas échéant;
- (d) Description des opérations de maintenance effectuées; et
- (e) Liste de l'équipement retiré ou remplacé (incluant les numéros d'identification, le cas échéant).

(2) L'organisation utilise des mécanismes automatisés pour planifier, exécuter, diriger et documenter les opérations de maintenance et de réparation et produire des dossiers à jour, précis, complets et facilement accessibles des opérations requises, en cours et terminées.

Références :

Aucune.

MA-3 OUTILS DE MAINTENANCE

Contrôle :

(A) L'organisation approuve, contrôle et maintient en permanence les outils de maintenance des systèmes d'information et en surveille l'utilisation.

Conseils supplémentaires : Le but de ce contrôle est de traiter les problèmes de sécurité liés à l'importation de matériel et de logiciel dans le système d'information aux fins de diagnostic et de réparation (p. ex., matériel ou logiciel renifleur de paquet installé pour remplir une fonction de maintenance particulière). Les composantes matérielles et (ou) logicielles qui servent à la maintenance du système, bien qu'elles en font partie (p. ex., logiciel utilisé pour exécuter les fonctions « ping », « ls » ou « ipconfig », ou matériel et logiciel servant de port de surveillance de commutateur Ethernet), sont hors de la portée de ce contrôle. Contrôle connexe : MP-6.

Améliorations du contrôle :

(1) L'organisation inspecte tous les outils introduits dans une installation par le personnel de maintenance à des fins de modifications inappropriées.

Conseils supplémentaires d'amélioration : Les outils de maintenance incluent, par exemple, l'équipement de diagnostic et de test servant à la maintenance du système.

(2) L'organisation vérifie que les supports qui contiennent des programmes de diagnostic et de test sont exempts de code malveillant avant de les utiliser dans le système.

(3) L'organisation prévient les retraits non autorisés d'équipement de maintenance; à cette fin, soit elle (i) vérifie que l'équipement ne contient aucune information organisationnelle, (ii) nettoie et détruit l'équipement, (iii) conserve l'équipement dans l'installation ou (iv) obtient une exemption d'un agent désigné l'autorisant explicitement à retirer l'équipement de l'installation.

(4) L'organisation utilise des mécanismes automatisés pour restreindre l'utilisation des outils de maintenance au seul personnel autorisé.

Références :

Aucune.

MA-4 MAINTENANCE EFFECTUÉE À DISTANCE

Contrôle :

(A) L'organisation autorise, surveille et contrôle les activités de maintenance et de diagnostic effectuées à distance.

(B) L'organisation permet l'utilisation des outils servant à cette fin seulement si elle est conforme à sa politique et documentée dans le plan de sécurité du système d'information.

(C) L'organisation utilise des techniques d'identification et d'authentification robustes lors de l'établissement des sessions d'activités de maintenance et de diagnostic effectuées à distance.

(D) L'organisation tient à jour des dossiers de ces activités.

(E) [Voir la section Améliorations du contrôle.]

Conseils supplémentaires : Les activités de maintenance et de diagnostic effectuées à distance sont des activités exécutées par des personnes connectées au système par un réseau externe (p. ex., Internet) ou interne. Les activités de maintenance et de diagnostic locales sont effectuées par des employés situés dans les locaux qui hébergent le système ou ses composantes et qui ne communiquent pas par une connexion réseau. Les techniques d'identification et d'authentification utilisées lors de l'établissement des sessions d'activités de maintenance et de diagnostic effectuées à distance sont conformes aux exigences d'accès aux réseaux énoncées dans le contrôle IA-2. Les authentifiants robustes incluent, par exemple, la technologie ICP dont les certificats sont stockés dans un jeton protégé par mot de passe, une phrase passe ou des données biométriques. L'application des exigences énoncées dans le contrôle MA-4 est effectuée en partie par d'autres contrôles. Contrôles connexes : AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-8, MA-5, MP-6, SC-7.

Améliorations du contrôle :

(1) L'organisation vérifie les sessions d'activités de maintenance et de diagnostic effectuées à distance, et des responsables désignés examinent les dossiers de maintenance des sessions.

(2) L'organisation documente, dans le plan de sécurité du système, l'installation et l'utilisation de ces connexions.

(3) L'organisation :

- (a) Exige que les services de maintenance et de diagnostic soient effectués à partir d'un système qui applique un niveau de sécurité aussi élevé que celui du système cible; ou
- (b) Retire la composante concernée du système avant l'exécution des activités de maintenance et de diagnostic, la nettoie (en supprime toute information organisationnelle) avant de l'expédier à l'extérieur et, une fois les services exécutés, l'inspecte et la nettoie à nouveau (pour en éliminer tout logiciel malveillant et implant indétectable) avant de la reconnecter au système d'information.

(4) L'organisation protège ces activités en utilisant un authentifiant robuste étroitement lié à l'utilisateur; elle isole également la session de maintenance des autres sessions de réseau du système, comme suit :

- (a) Elle sépare physiquement les voies de communication, ou
- (b) Elle sépare logiquement les voies de communication en recourant à une méthode de chiffrement conforme aux exigences du contrôle SC-13.

Conseils supplémentaires d'amélioration : Contrôle connexe : SC-13.

(5) L'organisation exige :

(a) Que le personnel chargé de la maintenance informe [*Affectation : liste des employés définie par l'organisation*] du moment où les activités sont prévues (c.-à-d., l'heure et la date); et

(b) Qu'un agent désigné de l'organisation, possédant des connaissances spécifiques sur la sécurité de l'information et des systèmes d'information, approuve les activités de maintenance.

(6) L'organisation utilise des mécanismes cryptographiques pour protéger l'intégrité et la confidentialité des communications durant les activités.

(7) L'organisation vérifie la déconnexion à distance du réseau à la fin des sessions.

Conseils supplémentaires d'amélioration : Les activités de maintenance et de diagnostic effectuées à distance sont des activités exécutées par des personnes connectées au système par un réseau externe (p. ex., Internet) ou interne. Les activités de maintenance et de diagnostic locales sont effectuées par des employés situés dans les locaux qui hébergent le système ou ses composantes et qui ne communiquent pas par une connexion réseau. Les techniques d'identification et d'authentification utilisées lors de l'établissement des sessions d'activités de maintenance et de diagnostic effectuées à distance sont conformes aux exigences d'accès aux réseaux énoncées dans le contrôle IA-2. Les authentifiants robustes incluent, par exemple, la technologie ICP dont les certificats sont stockés dans un jeton protégé par mot de passe, une phrase passe ou des données biométriques. L'application des exigences énoncées dans le contrôle MA-4 est effectuée en partie par d'autres contrôles. Contrôles connexes : AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-8, MA-5, MP-6, SC-7.

Références :

Guide sur l'authentification des utilisateurs pour les systèmes TI (ITSG-31) du CSTC [Référence 19].

MA-5 PERSONNEL DE MAINTENANCE

Contrôle :

(A) L'organisation établit un processus d'autorisation du personnel de maintenance et tient à jour une liste des organisations et des employés autorisés à effectuer ces activités.

(B) L'organisation s'assure que le personnel de maintenance possède les autorisations d'accès requises ou désigne un employé de l'organisation qui possède cette autorisation ainsi que les compétences techniques nécessaires pour superviser les travaux.

Conseils supplémentaires : Les personnes non identifiées au préalable dans le système d'information, tels les employés d'un fournisseur ou des consultants, peuvent légitimement demander un accès privilégié, par exemple, pour effectuer des activités de maintenance ou de diagnostic avec très peu de préavis ou sans préavis. Après une évaluation préalable des risques, l'organisation peut émettre des justificatifs d'identité temporaires à ces individus. Ces justificatifs peuvent être émis pour un seul accès ou pour une période de temps très limitée. Contrôles connexes : IA-8, MA-5.

Améliorations du contrôle :

(1) L'organisation a prévu des procédures pour le personnel de maintenance qui ne possède pas les cotes de sécurité appropriées ou qui n'est pas citoyen canadien; ces procédures incluent les exigences suivantes :

(a) Le personnel qui ne possède pas les autorisations d'accès, les cotes de sécurité ou les approbations formelles d'accès requises est escorté et surveillé durant l'exécution des activités de maintenance et de diagnostic par des employés de l'organisation techniquement qualifiés et autorisés et qui possèdent les cotes de sécurité et les autorisations d'accès appropriées;

(b) Avant que ce personnel puisse entreprendre les activités de maintenance ou de diagnostic, toutes les composantes de stockage d'information volatile du système sont nettoyées, et les supports d'information non volatile sont enlevés ou physiquement déconnectés du système puis rangés dans un endroit sûr; et

(c) Dans l'éventualité où une composante ne peut être nettoyée, l'organisation applique les procédures prévues dans le plan de sécurité du système.

Conseils supplémentaires d'amélioration : Le but de cette amélioration de contrôle est d'interdire, aux individus qui ne possèdent pas les cotes de sécurité appropriées (c.-à-d., qui ne possèdent pas de cote ou dont la cote est inférieure au

niveau de sécurité requis) ou qui ne sont pas citoyens canadiens, tout accès visuel et électronique à quelque renseignement classifié ou protégé que ce soit du système. Les procédures concernant l'utilisation du personnel de maintenance peuvent être documentées dans le plan de sécurité du système.

(2) L'organisation s'assure que les personnes qui effectuent la maintenance et le diagnostic des fonctions de traitement, de stockage et de transmission de l'information classifiée d'un système possèdent une cote de sécurité de niveau équivalent au niveau le plus élevé de confidentialité de l'information contenue dans les systèmes.

(3) L'organisation s'assure que les personnes qui effectuent la maintenance et le diagnostic des fonctions de traitement, de stockage et de transmission de l'information classifiée d'un système sont des citoyens canadiens.

(4) L'organisation s'assure que :

(a) Des ressortissants étrangers possédant une cote de sécurité appropriée sont utilisés pour exécuter les activités de maintenance et de diagnostic d'un système seulement lorsque celui-ci est possédé et exploité à la fois par le gouvernement canadien et des gouvernements étrangers alliés, ou uniquement par des gouvernements étrangers alliés; et

(b) Les approbations, les consentements et les modalités opérationnelles détaillées concernant l'utilisation de ces ressortissants sont bien documentés dans un protocole d'entente.

Références :

Vendor Support for Security Products (ITSA-23) du CSTC [Référence 31].

MA-6 MAINTENANCE OPPORTUNE

Contrôle :

(A) L'organisation obtient des services de maintenance et (ou) des pièces de rechange pour [*Affectation : liste définie par l'organisation des composantes de sécurité critiques de système et (ou) de composantes clés de technologie de l'information*] dans les [*Affectation : durée définie par l'organisation*] qui suivent la panne.

Conseils supplémentaires : L'organisation identifie les composantes de système qui, lorsqu'elles ne sont pas opérationnelles, posent des risques de sécurité accrus aux organisations, aux individus ou au Canada puisqu'elles ne sont pas en mesure de remplir leurs fonctions de sécurité. Les composantes de sécurité critiques incluent, par exemple, les pare-feu, les passerelles, les systèmes de détection d'intrusions, les dépôts de vérification, les serveurs d'authentification et les systèmes de prévention des intrusions. Contrôle connexe : CP-2.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

4.10 FAMILLE : PROTECTION DES SUPPORTS

CLASSE : OPÉRATIONNELLE

MP-1 POLITIQUE ET PROCÉDURES DE PROTECTION DES SUPPORTS

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique de protection des supports formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de protection des supports et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de protection des supports. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique de protection des supports peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures de protection des supports peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique de protection des supports. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7].
*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].
Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].

MP-2 ACCÈS AUX SUPPORTS

Contrôle :

(A) L'organisation restreint l'accès des [*Affectation : types de support numérique et non numérique définis par l'organisation*] aux [*Affectation : liste des personnes autorisées définie par l'organisation*] en conformité avec [*Affectation : mesures de sécurité définies par l'organisation*].

Conseils supplémentaires : Les supports utilisés pour les systèmes d'information incluent à la fois les supports numériques (p. ex., disquettes, bandes magnétiques, disques rigides externes et (ou) amovibles, clés USB, disques compacts et vidéodisques numériques) et non numériques (papier, microfilm, etc.). Ce contrôle s'applique également à l'informatique mobile et aux dispositifs de communications dotés d'une capacité de stockage d'information (p. ex., portables, assistants numériques, téléphones cellulaires, caméras numériques et matériel d'enregistrement sonore). Une évaluation organisationnelle des risques permet de déterminer les supports, et

l'information qu'ils contiennent, qui requièrent un accès restreint. Les organisations documentent dans les politiques et procédures les supports qui requièrent un accès restreint, les employés autorisés à y accéder et les mesures spécifiques de restriction d'accès. Peu de mesures de protection sont requises dans le cas des supports qui contiennent de l'information qui, selon l'organisation, est du domaine public, peut être diffusée publiquement ou dont l'accès par du personnel non autorisé n'a aucune ou peu d'incidence négative. Dans ces derniers cas, on présume que les contrôles d'accès physique des lieux où sont conservés les supports offrent une protection adéquate. Contrôles connexes : MP-4, PE-3.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour restreindre l'accès aux locaux d'entreposage des supports et vérifier les tentatives d'accès ainsi que les droits d'accès accordés.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle s'applique principalement aux locaux d'entreposage des supports où est remisé un volume important de supports et ne s'applique pas à tous les emplacements où sont conservés certains supports (p. ex., bureaux individuels).

(2) Le système utilise des mécanismes cryptographiques pour protéger et restreindre l'accès aux supports numériques portables.

Références :

Aucune.

MP-3 MARQUAGE DES SUPPORTS

Contrôle :

(A) L'organisation, en conformité avec ses politiques et procédures, appose sur les supports amovibles et les sorties des systèmes d'information des indications sur les limites de distribution, les mises en garde concernant la manipulation et l'étiquetage de sécurité (le cas échéant) de l'information.

(B) L'organisation exempte les [*Affectation : liste définie par l'organisation des types de support amovible*] de tout marquage pour autant qu'ils demeurent dans [*Affectation : locaux contrôlés définis par l'organisation*].

Conseils supplémentaires : Le terme marquage est utilisé pour désigner l'application ou l'utilisation d'attributs de sécurité lisibles par des humains. Le terme étiquetage est utilisé pour désigner l'application ou l'utilisation d'attributs de sécurité liés aux structures de données internes du système (voir le contrôle AC-16, Attributs de sécurité). Les supports amovibles incluent à la fois les supports numériques (p. ex., disquettes, bandes magnétiques, disques rigides externes et (ou) amovibles, clés USB, disques compacts, vidéodisques numériques) et non numériques (papier, microfilm, etc.). Une évaluation organisationnelle des risques permet de déterminer les supports qui requièrent un marquage. Le marquage n'est généralement pas requis dans le cas des supports qui contiennent de l'information qui, selon l'organisation, est du domaine public ou peut être diffusée publiquement. Certaines organisations, toutefois, peuvent exiger le marquage de l'information publique pour indiquer qu'elle peut être diffusée publiquement. Les organisations peuvent étendre la portée de ce contrôle et inclure les dispositifs de sortie qui contiennent de l'information organisationnelle, par exemple, les moniteurs et les imprimantes. Le marquage des supports amovibles et des sorties des systèmes est conforme aux lois du GC et aux politiques, directives et normes concernées du SCT.

Améliorations du contrôle :

Aucune.

Références :

Norme Sécurité relative à l'organisation et l'administration du SCT [Référence 14].

MP-4 ENTREPOSAGE DES SUPPORTS

Contrôle :

(A) L'organisation contrôle physiquement et entrepose de manière sécuritaire les [*Affectation : types de support numérique et non numérique définis par l'organisation*] dans [*Affectation : locaux contrôlés définis par l'organisation*], en conformité avec le *Guide d'équipement de sécurité (G1-001) de la GRC* [Référence 16].

(B) L'organisation protège physiquement et entrepose de manière sécuritaire les supports de système d'information classifiée et protégée en attente de leur destruction (sur place ou à l'extérieur) en utilisant de l'équipement, des techniques et des procédures approuvés.

Conseils supplémentaires : Les supports utilisés pour les systèmes d'information incluent à la fois les supports numériques (p. ex., disquettes, bandes magnétiques, disques rigides externes et (ou) amovibles, clés USB, disques compacts, vidéodisques numériques) et non numériques (papier, microfilm, etc.). Ce contrôle s'applique également à l'informatique mobile et aux dispositifs de communications dotés d'une capacité de stockage d'information (p. ex., portables, assistants numériques, téléphones cellulaires, caméras numériques et matériel d'enregistrement sonore). Les systèmes téléphoniques sont également considérés des systèmes d'information et peuvent stocker de l'information dans des supports internes (p. ex., systèmes de messagerie vocale). Puisque ces systèmes ne sont pas, dans la plupart des cas, dotés des mécanismes d'identification, d'authentification et de contrôle d'accès normalement utilisés dans d'autres systèmes d'information, le personnel de l'organisation doit être très vigilant quant aux types d'information stockés dans les systèmes de messagerie vocale téléphoniques. Une zone contrôlée est toute zone ou emplacement dont l'organisation juge les mesures de protection physiques et procédurales suffisantes pour satisfaire aux exigences actuelles de protection de l'information et (ou) des systèmes.

Une évaluation organisationnelle permet de déterminer les supports, et l'information qu'ils contiennent, qui requièrent une protection physique. Moins de mesures de protection sont requises dans le cas des supports qui contiennent de l'information qui, selon l'organisation, est du domaine public, peut être diffusée publiquement ou dont l'accès par du personnel non autorisé n'a aucune ou peu d'incidence négative sur les activités et les biens de l'organisation, sur les individus, les autres organisations ou le Canada. Dans ces derniers cas, on présume que les contrôles d'accès physique des endroits où sont conservés les supports offrent une protection adéquate.

Dans le contexte de la stratégie de défense en profondeur, l'organisation envisagera habituellement de recourir au chiffrement de l'information inactive contenue dans certains dispositifs de stockage secondaires. Le recours à la cryptographie est à la discrétion du propriétaire et (ou) du gardien de l'information. Le choix des mécanismes cryptographiques est lié à la préservation de la confidentialité et de l'intégrité de l'information. La force des mécanismes correspond à la classification et à la sensibilité de l'information. Contrôles connexes : AC-3, AC-19, CP-6, CP-9, MP-2, PE-3.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes cryptographiques pour protéger l'information entreposée.

Conseils supplémentaires d'amélioration : Contrôle connexe : SC-13.

Références :

Guide d'équipement de sécurité (G1-001) de la GRC [Référence 16],
Effacement et déclassification des supports d'information électroniques (ITSG-06) du CSTC [Référence 17].
Pièces sécuritaires (G1-029) de la GRC [Référence 24].

MP-5 TRANSPORT DES SUPPORTS

Contrôle :

(A) L'organisation protège et contrôle [*Affectation : types de support numérique et non numérique définis par l'organisation*] durant leur transport hors des zones contrôlées en utilisant [*Affectation : mesures de sécurité définies par l'organisation*] en conformité avec la *Norme opérationnelle sur la sécurité matérielle du SCT* [Référence 7] et la *Norme pour le transport ou la transmission de renseignements et de biens de nature délicate (G1-009) de la GRC* [Référence 18].

(B) L'organisation demeure responsable des supports durant leur transport hors des zones contrôlées.

(C) L'organisation réserve les activités associées au transport de ces supports au personnel autorisé.

Conseils supplémentaires : Les supports utilisés pour les systèmes d'information incluent à la fois les supports numériques (p. ex., disquettes, bandes magnétiques, disques rigides externes et (ou) amovibles, clés USB, disques compacts, vidéodisques numériques) et non numériques (papier, microfilm, etc.). Ce contrôle s'applique également à l'informatique mobile et aux dispositifs de communications dotés d'une capacité de stockage d'information (p. ex., portables, assistants numériques, téléphones cellulaires, caméras numériques et matériel d'enregistrement sonore). Les systèmes téléphoniques sont également considérés des systèmes d'information et peuvent stocker de l'information dans des supports internes (p. ex., systèmes de messagerie vocale). Puisque ces systèmes ne sont pas, dans la plupart des cas, dotés des mécanismes d'identification, d'authentification et de contrôle d'accès normalement utilisés dans d'autres systèmes d'information, le personnel de l'organisation doit être très vigilant quant aux types d'information stockés dans les systèmes de messagerie vocale téléphoniques qui sont transportés hors des zones contrôlées. Une zone contrôlée est toute zone ou emplacement dont l'organisation juge les mesures de protection physiques et procédurales suffisantes pour satisfaire aux exigences actuelles de protection de l'information et (ou) des systèmes d'information.

Les mesures de sécurité physique et technique de protection des supports numériques et non numériques correspondent à la classification ou à la sensibilité de l'information qu'ils contiennent et sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les conteneurs verrouillés et la cryptographie sont des exemples de mesures de sécurité qui permettent de protéger les supports numériques et non numériques durant leur transport. Certains mécanismes cryptographiques peuvent protéger la confidentialité et (ou) l'intégrité de l'information. Une évaluation organisationnelle des risques permet de déterminer les supports, et l'information qu'ils contiennent, qui requièrent une protection durant leur transport, et de choisir les conteneurs de stockage utilisés pour transporter les supports non numériques. Le personnel autorisé responsable du transport et de la messagerie peut inclure des individus de l'extérieur de l'organisation (p. ex., Postes Canada ou service de transport ou de livraison commercial). Contrôles connexes : AC-19, CP-9.

Améliorations du contrôle :

(1) [Annulée : voir le contrôle MP-5].

(2) L'organisation documente les activités associées au transport des supports.

Conseils supplémentaires d'amélioration : Les organisations établissent les exigences de documentation des activités associées au transport des supports en conformité avec l'évaluation organisationnelle des risques. Ces exigences peuvent inclure la capacité de définir différentes méthodes de documentation du transport pour différents types de support.

(3) L'organisation fait appel à un gardien désigné durant le transport des supports.

Conseils supplémentaires d'amélioration : Les responsabilités qui incombent au gardien peuvent être transférées d'un individu à l'autre pour autant qu'il n'y ait à aucun moment d'ambiguïté quant à l'identité du gardien.

(4) L'organisation utilise des mécanismes cryptographiques conformes aux exigences du contrôle SC-13 pour protéger la confidentialité et l'intégrité de l'information stockée dans des supports numériques durant leur transport hors des zones contrôlées.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle s'applique également aux dispositifs mobiles. Les dispositifs mobiles incluent les supports de stockage portables (p. ex., clés USB, lecteurs de disque rigides externes) et les dispositifs de communications et de traitement portables dotés d'une capacité de stockage (p. ex., portables, assistants numériques, téléphones cellulaires). Contrôles connexes : SC-13.

Références :

Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7].
Norme pour le transport ou la transmission de renseignements et de biens de nature délicate (G1-009) de la GRC [Référence 18].
Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés (ITSA-11D) du CSTC [Référence 9].
Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B (ITSB-40) du CSTC [Référence 29].
Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].

MP-6 NETTOYAGE DES SUPPORTS

Contrôle :

(A) L'organisation nettoie les supports numériques et non numériques de système d'information avant leur élimination ou leur transfert hors de son contrôle ou à des fins de réutilisation.

(B) L'organisation utilise des mécanismes de nettoyage dont la force et l'intégrité correspondent à la classification ou à la sensibilité de l'information.

Conseils supplémentaires : Ce contrôle s'applique à tous les supports susceptibles d'être éliminés ou réutilisés, qu'ils soient amovibles ou non. Le nettoyage est le processus qui consiste à supprimer l'information des supports de manière que l'organisation puisse être raisonnablement assurée que l'information ne peut être extraite ou reconstruite. Les nettoyages techniques, incluant l'effacement, l'épuration et la destruction de l'information contenue dans les supports, empêche la divulgation d'information organisationnelle à des personnes non autorisées lorsque les supports sont réutilisés ou transférés aux fins d'élimination. L'organisation utilise à sa discrétion les techniques et procédures de nettoyage des supports qui contiennent de l'information du domaine public, ou qui peut être diffusée publiquement, ou dont le transfert à des fins de réutilisation ou d'élimination n'a pas d'incidence négative sur l'organisation ou les individus. Contrôles connexes : MP-4, MP-5.

Améliorations du contrôle :

(1) L'organisation piste, documente et vérifie le nettoyage des supports et les activités d'élimination.

(2) L'organisation teste les procédures et l'équipement de nettoyage pour s'assurer de leur bon rendement [*Affectation : fréquence définie par l'organisation*].

(3) L'organisation nettoie les dispositifs portables et amovibles avant de les connecter au système d'information dans les situations suivantes : [*Affectation : liste définie par l'organisation des circonstances où les dispositifs de stockage portables et amovibles doivent être nettoyés*].

Conseils supplémentaires d'amélioration : Les dispositifs de stockage portables et amovibles (p. ex., clés USB, dispositifs de stockage externes) peuvent être la source d'insertions de code malveillant dans les systèmes organisationnels. Plusieurs de ces dispositifs proviennent de sources inconnues et peuvent contenir divers types de code malveillant susceptibles d'être transmis au système par des ports USB ou d'autres portails d'entrée. On recommande de toujours analyser ces dispositifs; toutefois, le nettoyage offre une assurance supplémentaire qu'ils sont exempts de tout code malveillant, incluant le code capable de lancer des attaques du jour zéro. Les organisations jugent utile de nettoyer ces dispositifs, par exemple, au moment de l'achat chez un fabricant ou un fournisseur et avant leur utilisation, ou lorsqu'il y a interruption de leur chaîne de possession. Une évaluation organisationnelle des risques permet de déterminer les circonstances particulières où on doit recourir au processus de nettoyage. Contrôle connexe : SI-3.

(4) L'organisation nettoie les supports qui contiennent de l'information sensible en conformité avec les politiques, normes et procédures pertinentes du GC.

(5) L'organisation nettoie les supports qui contiennent de l'information classifiée en conformité avec les normes et politiques du CSTC.

(6) L'organisation détruit les supports qui ne peuvent être nettoyés.

Références :

Guide d'équipement de sécurité (G1-001) de la GRC [Référence 16].
Effacement et déclassification des supports d'information électroniques (ITSG-06) du CSTC [Référence 17].
Produits de réécriture des supports de TI et d'effacement sécurisé (B2-002) de la GRC [Référence 45].
Lignes directrices sur l'élimination et la destruction des renseignements protégés sur disques durs (G2-003) de la GRC [Référence 55].
Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].

4.11 FAMILLE : PROTECTION PHYSIQUE ET ENVIRONNEMENTALE

CLASSE : OPÉRATIONNELLE

PE-1 POLITIQUE ET PROCÉDURES DE PROTECTION PHYSIQUE ET ENVIRONNEMENTALE

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique de protection physique et environnementale formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de protection physique et environnementale et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de protection physique et environnementale. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique de protection physique et environnementale peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures de protection physique et environnementale peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique de protection physique et environnementale. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7].
*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].
Protection, détection et intervention (G1-025) de la GRC [Référence 52].

PE-2 AUTORISATIONS D'ACCÈS PHYSIQUE

Contrôle :

(A) L'organisation développe et tient à jour une liste des employés autorisés à accéder à l'installation qui héberge le système d'information (sauf dans les cas où l'installation est officiellement accessible au public).

(B) L'organisation émet des justificatifs d'autorisation.

(C) L'organisation examine et approuve la liste d'accès et les justificatifs [*Affectation : fréquence définie par l'organisation*], et supprime de la liste les employés qui n'ont plus besoin de droit d'accès.

Conseils supplémentaires : Les justificatifs d'autorisation incluent, par exemple, les badges, les cartes d'identité et les cartes à puce. Contrôles connexes : PE-3, PE-4.

Améliorations du contrôle :

(1) L'organisation autorise, selon le poste ou le rôle de l'employé, l'accès physique à l'installation qui héberge le système d'information.

(2) L'organisation exige deux formes d'identification pour permettre l'accès à l'installation.

Conseils supplémentaires d'amélioration : Exemples de formes d'identification : badge, carte-clé, NIP encodé et données biométriques.

(100) L'organisation émet à tout le personnel une carte d'identité qui inclut, au minimum, le nom de l'organisation, la photo et le nom du titulaire, un numéro de carte unique et une date d'expiration.

Références :

Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7].
Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].
Guide pour la préparation d'un énoncé de sécurité matérielle (G1-005) de la GRC [Référence 46].
Cartes d'identité / Insignes d'accès (G1-006) de la GRC [Référence 47].
Contrôle de l'accès (G1-024) de la GRC [Référence 51].
Protection, détection et intervention (G1-025) de la GRC [Référence 52].

PE-3 CONTRÔLE D'ACCÈS PHYSIQUE

Contrôle :

(A) L'organisation applique les autorisations d'accès physique à tous les points d'accès physique (incluant les points d'entrée/sortie désignés) de l'installation qui héberge le système d'information (à l'exclusion des zones de l'installation officiellement désignées accessibles au public).

(B) L'organisation vérifie les autorisations d'accès individuelles avant d'accorder l'accès à l'installation.

(C) L'organisation contrôle les entrées de l'installation qui héberge le système d'information en recourant à des dispositifs de contrôle d'accès physique et (ou) à des agents de sécurité.

(D) L'organisation contrôle l'accès aux zones officiellement désignées accessibles au public en conformité avec les directives d'évaluation des risques de l'organisation.

(E) L'organisation protège les clés, les combinaisons et autres dispositifs de contrôle d'accès physique.

(F) L'organisation maintient l'inventaire des dispositifs de contrôle d'accès physique [*Affectation : fréquence définie par l'organisation*].

(G) L'organisation modifie les combinaisons et les clés [*Affectation : fréquence définie par l'organisation*] lorsque des clés sont perdues, des combinaisons, compromises, ou lorsque des employés sont transférés ou quittent leur poste.

Conseils supplémentaires : Le contrôle de l'accès aux zones d'accès restreint et autres locaux de l'organisation doit être effectué de manière à ne pas contrevenir aux exigences relatives à la sécurité des personnes énoncées dans le Code national du bâtiment (CNB) 2005 [Référence 20], le Code national de prévention des incendies (CNPI) 2005 [Référence 21] et autres codes, normes et lignes directrices connexes. Se reporter au document Éléments du Code national du bâtiment 1995 touchant la sécurité (G1-007) de la GRC [Référence 22] pour plus de détails.

L'organisation détermine les types d'agent de sécurité appropriés, par exemple, des professionnels de la sécurité physique ou autres personnes tels des employés de l'administration ou des utilisateurs du système d'information. Les dispositifs de contrôle d'accès physique incluent, par exemple, les clés, les cadenas, les combinaisons et les lecteurs de cartes. Les postes de travail et les périphériques associés (et intégrés) à un système d'information

organisationnel peuvent être situés dans des zones désignées accessibles au public et doivent être assujettis à des mesure de protection. Contrôles connexes : MP-2, MP-4, PE-2.

Améliorations du contrôle :

(1) L'organisation applique les autorisations d'accès physique au système indépendamment des contrôles d'accès physique de l'installation.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle s'applique aux salles des serveurs, aux zones d'entreposage des supports, aux centres de communications ou à toute autre zone de l'installation qui héberge d'importantes concentrations de composantes. Le but de cette amélioration est d'offrir une sécurité physique supplémentaire dans les zones potentiellement plus vulnérables en raison de la concentration de composantes. Les exigences en matière de contrôle de sécurité des installations où se trouvent des systèmes organisationnels qui traitent, stockent ou transmettent de l'information sensible cloisonnée SCI (*Renseignements cloisonnés de nature délicate*[1]) sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Voir également le contrôle PS-3 sur les exigences de contrôle de sécurité concernant les accès du personnel à l'information sensible cloisonnée SCI.

(2) L'organisation effectue des vérifications de sécurité au périmètre physique de l'installation ou du système d'information pour détecter toute exfiltration non autorisée d'information ou de composante.

Conseils supplémentaires d'amélioration : L'ampleur, la fréquence ou la nature aléatoire des vérifications sont jugées nécessaires par l'organisation pour atténuer de manière adéquate les risques associés aux exfiltrations.

(3) L'organisation protège et surveille, 24 heures par jour et 7 jours par semaine, tous les points d'accès physique de l'installation qui héberge le système d'information et émet des alarmes, le cas échéant.

(4) L'organisation utilise des contenants verrouillables pour protéger [*Affectation : composantes de système définies par l'organisation*] contre les accès physiques non autorisés.

(5) Le système détecte et (ou) empêche le trafiquage physique ou l'altération des composantes matérielles.

(6) L'organisation utilise un processus de test de pénétration qui inclut [*Affectation : fréquence définie par l'organisation*] tentatives inopinées de contournement des contrôles de sécurité associés aux points d'accès physique de l'installation.

Conseils supplémentaires d'amélioration : Contrôle connexe : CA-2.

Références :

Manuel de la sécurité industrielle de TPSGC [Référence 3].
Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7].
Code national du bâtiment (CNB) 2005 [Référence 20].
Code national de prévention des incendies (CNPI) 2005 [Référence 21].
Éléments du Code national du bâtiment 1995 touchant la sécurité (G1-007) de la GRC [Référence 22].
Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].
Guide pour la préparation d'un énoncé de sécurité matérielle (G1-005) de la GRC [Référence 46].
Scellage de protection des clés d'urgence et passe-partout ou des serrures à code d'immeubles (G1-007) de la GRC [Référence 48].
Lignes directrices visant les services de gardiens (G1-008) de la GRC [Référence 49].
Les systèmes de clés maitresses (G1-016) de la GRC [Référence 50].
Contrôle de l'accès (G1-024) de la GRC [Référence 51].
Protection, détection et intervention (G1-025) de la GRC [Référence 52].
Établissement des zones de sécurité matérielle (G1-026) de la GRC [Référence 53].
Pièces sécuritaires (G1-029) de la GRC [Référence 24].
Protection matérielle des serveurs informatiques (G1-031) de la GRC [Référence 54].

---

[1] Le terme *information sensible cloisonnée* (SCI) désigne l'information classifiée pour laquelle le besoin de connaître est assujetti à des exigences supplémentaires. Le niveau de classification COMINT est un exemple de désignation SCI. Les employés dont la cote de sécurité et le besoin de savoir justifient un accès à l'information de niveau SCI doivent être soumis à des procédures supplémentaires de filtrage de sécurité (p. ex., un cours d'endoctrinement).

PE-4 CONTRÔLE D'ACCÈS AUX SUPPORTS DE TRANSMISSION

Contrôle :

(A) L'organisation contrôle l'accès physique aux lignes de distribution et de transmission des systèmes d'information dans ses installations.

Conseils supplémentaires : Les mesures de protection physiques appliquées aux lignes de distribution et de transmission des systèmes permettent de prévenir les dommages accidentels, les interruptions et le trafiquage physique. En plus, elles sont nécessaires pour aider à prévenir l'écoute clandestine ou la modification en temps réel des transmissions non chiffrées. Les mesures protectrices utilisées pour le contrôle accès physique incluent les suivantes : (i) verrouillage des cabinets de câblage, (ii) déconnexion ou verrouillage des connecteurs non utilisés et (ou) (iii) protection du câblage par des conduits ou des chemins de câbles. Contrôle connexe : PE-2.

Améliorations du contrôle :

Aucune.

Références :

Guide pour la préparation d'un énoncé de sécurité matérielle (G1-005) de la GRC [Référence 46].
Établissement des zones de sécurité matérielle (G1-026) de la GRC [Référence 53].

PE-5 CONTRÔLE D'ACCÈS AUX DISPOSITIFS DE SORTIE

Contrôle :

(A) L'organisation contrôle l'accès physique aux dispositifs de sortie de système d'information pour empêcher les personnes non autorisées d'obtenir les sorties.

Conseils supplémentaires : Les moniteurs, imprimantes et dispositifs audio sont des exemples de dispositifs de sortie.

Améliorations du contrôle :

Aucune.

Références :

Établissement des zones de sécurité matérielle (G1-026) de la GRC [Référence 53].

PE-6 SURVEILLANCE DE L'ACCÈS PHYSIQUE

Contrôle :

(A) L'organisation surveille l'accès physique au système d'information afin de détecter les incidents de sécurité physique et d'y répondre.

(B) L'organisation examine les journaux d'accès physique [*Affectation : fréquence définie par l'organisation*].

(C) L'organisation coordonne les résultats des examens et des enquêtes avec sa capacité d'intervention en cas d'incident.

Conseils supplémentaires : Les enquêtes et les interventions liées aux incidents de sécurité physique, incluant les violations de sécurité apparentes et les activités suspectes, font partie de la capacité d'intervention en cas d'incident de l'organisation.

Améliorations du contrôle :

(1) L'organisation surveille en temps réel les alarmes d'intrusion physique et l'équipement de surveillance.

(2) L'organisation utilise des mécanismes automatisés pour identifier les intrusions potentielles et lancer les opérations d'intervention prévues. Cette amélioration peut être implémentée par l'utilisation d'un système de détection d'intrusion qui amorce une réponse manuelle (p.ex., un commissionnaire investigue la cause d'une alarme).

Références :

Protection, détection et intervention (G1-025) de la GRC [Référence 52].

PE-7 CONTRÔLE DES VISITEURS

Contrôle :

(A) L'organisation contrôle l'accès physique au système d'information en authentifiant les visiteurs avant d'émettre une autorisation d'accès à l'installation qui héberge le système d'information, sauf dans le cas des zones désignées accessibles au public.

Conseils supplémentaires : Les individus (employés de l'organisation, personnel contractuel et autres) qui possèdent des justificatifs d'autorisation permanents pour l'installation ne sont pas considérés des visiteurs.

Améliorations du contrôle :

(1) L'organisation escorte les visiteurs et surveille leurs activités, le cas échéant.

(2) L'organisation exige deux formes d'identification pour permettre l'accès des visiteurs à l'installation.

Références :

Établissement des zones de sécurité matérielle (G1-026) de la GRC [Référence 53].

PE-8 DOSSIERS D'ACCÈS

Contrôle :

(A) L'organisation maintient des dossiers sur les visiteurs qui accèdent à l'installation où réside le système d'information (sauf dans les cas où l'installation est officiellement accessible au public).

(B) L'organisation examine les dossiers [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Les dossiers incluent, par exemple, le nom du visiteur et son organisation, sa signature, la ou les pièces d'identification, la date de l'accès, l'heure d'arrivée et de départ, le but de la visite et le nom de la personne ou de l'organisation visitée.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour faciliter la tenue à jour et l'examen des dossiers d'accès.

(2) L'organisation tient à jour un dossier de tous les accès physiques, tant des visiteurs que du personnel autorisé.

Références :

Aucune.

PE-9 ÉQUIPEMENT ET CÂBLAGE D' ALIMENTATION

Contrôle :

(A) L'organisation protège l'équipement et le câblage d'alimentation du système d'information contre les dommages et la destruction.

Conseils supplémentaires : Ce contrôle, et les améliorations correspondantes, peut être appliqué par une entité organisationnelle autre que celle responsable du programme de sécurité de l'information et qui satisfait à des exigences similaires. Les organisations doivent éviter la duplication des mesures de protection.

Améliorations du contrôle :

(1) L'organisation utilise des chemins de câblage d'alimentation redondants et parallèles.

(2) L'organisation utilise des contrôles de tension automatisés pour [*Affectation : liste définie par l'organisation des composantes essentielles de système*].

Références :

Aucune.

PE-10 ARRÊT D'URGENCE

Contrôle :

(A) L'organisation peut, en situations d'urgence, couper l'alimentation du système d'information ou des composantes individuelles.

(B) L'organisation place des interrupteurs ou des dispositifs d'arrêt d'urgence dans [*Affectation : liste définie par l'organisation des emplacements occupés par le système ou une composante*] pour faciliter l'accès en toute sécurité du personnel.

(C) L'organisation protège sa capacité d'interruption d'urgence de l'alimentation contre toute activation non autorisée.

Conseils supplémentaires : Ce contrôle s'applique aux installations qui contiennent des concentrations de ressources de système, par exemple, les centres de données, les salles de serveurs et les salles d'ordinateurs centraux.

Améliorations du contrôle :

(1) [Annulée : Intégrée au contrôle PE-10].

Références :

Aucune.

PE-11 ALIMENTATION D'URGENCE

Contrôle :

(A) L'organisation prévoit une source temporaire d'alimentation non interruptible pour faciliter l'arrêt ordonné du système d'information dans l'éventualité d'une perte de la source d'alimentation principale.

Conseils supplémentaires : Ce contrôle, et les améliorations correspondantes, peut être appliqué par une entité organisationnelle autre que celle responsable du programme de sécurité de l'information et qui satisfait à des exigences similaires. Les organisations doivent éviter la duplication des mesures de protection.

Améliorations du contrôle :

(1) L'organisation prévoit une source d'alimentation de secours à long terme capable de maintenir la capacité opérationnelle minimale requise dans l'éventualité d'une perte prolongée de la source d'alimentation principale.

(2) L'organisation prévoit une source d'alimentation de secours à long terme autonome et indépendante de toute source d'alimentation externe.

Conseils supplémentaires d'amélioration : Les sources d'alimentation de secours à long terme du système d'information sont activées manuellement ou automatiquement.

Références :

Aucune.

PE-12 ÉCLAIRAGE D'URGENCE

Contrôle :

(A) L'organisation utilise et entretient, pour le système d'information, un système automatique d'éclairage d'urgence qui entre en fonction lorsqu'il y a coupure ou interruption de courant; le système éclaire les sorties d'urgence et les chemins d'évacuation dans l'installation.

Conseils supplémentaires : Ce contrôle, et les améliorations correspondantes, peut être appliqué par une entité organisationnelle autre que celle responsable du programme de sécurité de l'information et qui satisfait à des exigences similaires. Les organisations doivent éviter la duplication des mesures de protection.

Améliorations du contrôle :

(1) L'organisation prévoit l'éclairage d'urgence de toutes les zones de l'installation où sont exécutées des fonctions opérationnelles et de mission essentielles.

Références :

Aucune.

PE-13 PROTECTION CONTRE LES INCENDIES

Contrôle :

(A) L'organisation utilise et maintient, pour le système d'information, des réseaux et (ou) des dispositifs de détection et d'extinction d'incendie branchés à une source d'alimentation indépendante.

Conseils supplémentaires : Les réseaux et (ou) dispositifs de détection et d'extinction d'incendie incluent, par exemple, les systèmes de gicleurs, les extincteurs manuels, les boyaux d'arrosage fixes et les détecteur de fumée. Ce contrôle, et les améliorations correspondantes, peut être appliqué par une entité organisationnelle autre que celle responsable du programme de sécurité de l'information et qui satisfait à des exigences similaires. Les organisations doivent éviter la duplication des mesures de protection.

Améliorations du contrôle :

(1) L'organisation utilise des réseaux et (ou) dispositifs de détection d'incendie qui entrent en fonction automatiquement et informe l'organisation et les intervenants d'urgence dans l'éventualité d'un incendie.

(2) L'organisation utilise des réseaux et (ou) dispositifs d'extinction d'incendie qui informent automatiquement l'organisation et les intervenants d'urgence dès qu'ils sont activés.

(3) L'organisation utilise un système d'extinction automatique d'incendie dans les installations où il n'y a pas de personnel permanent.

(4) L'organisation s'assure que l'installation fait l'objet [*Affectation : fréquence définie par l'organisation*] d'inspections du service des incendies et corrige rapidement toutes les lacunes relevées.

Références :

Aucune.

PE-14 CONTRÔLE DE LA TEMPÉRATURE ET DE L' HUMIDITÉ

Contrôle :

(A) L'organisation maintient à [*Affectation : niveaux acceptables définis par l'organisation*] les niveaux de température et d'humidité dans l'installation qui héberge le système d'information.

(B) L'organisation surveille les niveaux de température et d'humidité [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Ce contrôle, et les améliorations correspondantes, peut être appliqué par une entité organisationnelle autre que celle responsable du programme de sécurité de l'information et qui satisfait à des exigences similaires. Les organisations doivent éviter la duplication des mesures de protection.

Améliorations du contrôle :

(1) L'organisation utilise des contrôles automatiques de la température et de l'humidité pour empêcher toute fluctuation potentiellement préjudiciable.

(2) L'organisation utilise un processus de surveillance de la température et de l'humidité qui produit une alarme ou un avis en cas de changements potentiellement préjudiciables pour le personnel ou l'équipement.

Références :

Aucune.

PE-15 PROTECTION CONTRE LES DÉGÂTS D'EAU

Contrôle :

(A) L'organisation protège le système d'information contre tout dommage causé par une fuite d'eau en recourant à des vannes d'arrêt accessibles qui fonctionnent adéquatement et dont le personnel concerné connaît l'emplacement.

Conseils supplémentaires : Ce contrôle, et les améliorations correspondantes, peut être appliqué par une entité organisationnelle autre que celle responsable du programme de sécurité de l'information et qui satisfait à des exigences similaires. Les organisations doivent éviter la duplication des mesures de protection.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes capables, sans intervention manuelle, de protéger le système d'information contre tout dommage causé par une fuite d'eau éventuelle.

Références :

Aucune.

PE-16 LIVRAISON ET RETRAIT

Contrôle :

(A) L'organisation autorise, surveille et contrôle l'entrée et la sortie dans l'installation des [*Affectation : types de composante de système définis par l'organisation*] et tient à jour les dossiers pertinents.

Conseils supplémentaires : L'application réelle des autorisations d'entrée et de sortie des composantes peut exiger une restriction d'accès aux aires de livraison et, éventuellement, leur isolation du système et des zones d'entreposage des supports.

Améliorations du contrôle :

Aucune.

Références :

Contrôle de l'accès (G1-024) de la GRC [Référence 51].

PE-17 LIEU DE TRAVAIL DE SECOURS

Contrôle :

(A) L'organisation utilise [*Affectation : contrôles de sécurité de gestion, opérationnels et techniques de système définis par l'organisation*] dans les lieux de travail de secours.

(B) L'organisation évalue dans la mesure du possible l'efficacité des contrôles de sécurité dans les lieux de travail de secours.

(C) L'organisation permet aux employés de communiquer avec le personnel chargé de la sécurité de l'information en cas d'incidents ou de problèmes de sécurité.

Conseils supplémentaires : Les lieux de travail de secours peuvent inclure, par exemple, des installations du gouvernement ou des résidences privées d'employés. L'organisation peut définir différents ensembles de contrôles de sécurité pour des lieux de travail de secours ou des types de site spécifiques.

Améliorations du contrôle :

Aucune.

Références :

Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7].

PE-18 EMPLACEMENT DES COMPOSANTES DE SYSTÈME D'INFORMATION

Contrôle :

(A) L'organisation entrepose les composantes de système d'information de manière à réduire tout dommage potentiel de nature physique et environnementale et à réduire les risques d'accès non autorisé.

Conseils supplémentaires : Les dangers de nature physique et environnementale incluent, par exemple, les inondations, les incendies, les tornades, les tremblements de terre, les ouragans, les actes terroristes, le vandalisme, les impulsions électromagnétiques, les interférences électriques et les radiations électromagnétiques. Dans la mesure du possible, l'organisation choisit un emplacement ou un site en tenant compte de ces dangers. En plus, elle choisit l'emplacement des points d'entrée physique de manière à s'assurer qu'aucune personne non

autorisée, même si l'accès lui est interdit, ne puisse s'approcher du système d'information et accéder illégalement aux communications (p. ex., en utilisant des renifleurs ou des microphones sans fil). Ce contrôle, et les améliorations correspondantes, peut être appliqué par une entité organisationnelle autre que celle responsable du programme de sécurité de l'information et qui satisfait à des exigences similaires. Les organisations doivent éviter la duplication des mesures de protection.

Améliorations du contrôle :

(1) L'organisation planifie l'emplacement ou le site de l'installation qui héberge le système en tenant compte des dangers de nature physique et environnementale et, dans la cas des installations existantes, tient compte de ces dangers dans sa stratégie d'atténuation du risque.

Références :

Critères pour la conception, la fabrication, l'approvisionnement, l'installation et les essais de réception des enceintes blindées contre les radiofréquences (ITSG-02) du CSTC [Référence 36].
Établissement des zones de sécurité matérielle (G1-026) de la GRC [Référence 53].

PE-19 FUITES D'INFORMATION

Contrôle :

(A) L'organisation protège le système d'information contre les fuites d'information dues aux émissions d'ondes électromagnétiques.

Conseils supplémentaires : La catégorie de sécurité (confidentialité) du système d'information et la politique de sécurité de l'organisation permettent de cibler l'application des mesures de protection et des contremesures utilisées de manière à protéger le système contre les fuites d'information dues aux émissions d'ondes électromagnétiques.

Améliorations du contrôle :

(1) L'organisation s'assure que les composantes et les communications de données et les réseaux sont protégés en conformité avec (i) les politiques et procédures du GC en matière d'émissions et la norme TEMPEST, et (ii) la sensibilité de l'information transmise.

Références :

Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada (ITSD-01) du CSTC, [Référence 15].
Planification des installations COMSEC – Conseils et critères (ITSG-11) du CSTC [Référence 38].
Procédures d'évaluation des installations du gouvernement du Canada (ITSG-12) du CSTC [Référence 39].

4.12 FAMILLE : PLANIFICATION

CLASSE : GESTION

PL-1 POLITIQUE ET PROCÉDURES DE PLANIFICATION DE LA SÉCURITÉ

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique de planification de la sécurité formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de planification de la sécurité et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de permettre la création de la politique et des procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de planification de la sécurité. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique de planification de la sécurité traite des exigences stratégiques globales liées à la confidentialité, l'intégrité et la disponibilité et peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures de planification de la sécurité peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique de planification de la sécurité. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

PL-2 PLAN DE SÉCURITÉ DES SYSTÈMES

Contrôle :

(A) L'organisation développe pour le système d'information un plan de sécurité qui :

(a) Est conforme à l'architecture d'entreprise de l'organisation;

(b) Définit explicitement les limites d'autorisation du système;

(c) Décrit le contexte opérationnel du système au plan de la mission et des processus opérationnels;

(d) Définit les catégories de sécurité du système, incluant la logique sous-jacente;

(e) Décrit l'environnement opérationnel du système;

(f) Décrit les relations ou les connexions avec les autres systèmes;

(g) Donne un aperçu des exigences du contrôle de sécurité du système;

(h) Décrit les contrôles de sécurité existants ou prévus pour répondre à ces exigences, y compris la justification des décisions concernant l'adaptation des contrôles et l'identification des contrôles complémentaires; et

(i) Sera examiné et approuvé par le responsable de l'autorisation ou un représentant désigné avant la mise en œuvre du plan.

(B) L'organisation examine le plan de sécurité du système d'information [*Affectation : fréquence définie par l'organisation*].

(C) L'organisation met le plan à jour pour tenir compte des changements apportés au système et (ou) à l'environnement d'exploitation, ou des problèmes soulevés lors de la mise en œuvre du plan ou des évaluations des contrôles de sécurité.

Conseils supplémentaires : Le plan de sécurité contient suffisamment d'information (incluant la spécification explicite ou par référence des paramètres d'affectation et de sélection des contrôles) pour permettre une mise en œuvre formelle conforme à ses objectifs et l'identification éventuelle des risques qu'il représente, s'il est appliqué tel que prévu, pour les activités et les biens de l'organisation, les individus, les autres organisations et le Canada. Contrôles connexes : PM-1, PM-7, PM-8, PM-9, PM-11.

Améliorations du contrôle :

(1) L'organisation :

(a) Développe pour le système d'information un concept d'opération (CONOPS) de sécurité qui inclut, au minimum : (i) le but du système; (ii) une description de l'architecture du système; (iii) le barème d'autorisation de sécurité; et (iv) les catégories de sécurité et les facteurs utilisés pour les déterminer; et

(b) Révise et tient à jour le CONOPS [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires d'amélioration : Le CONOPS de sécurité peut être inclus dans le plan de sécurité du système.

(2) L'organisation développe pour le système d'information une architecture fonctionnelle qui identifie et maintient :

(a) Les interfaces externes, l'information échangée entre elles et leurs mécanismes de protection;

(b) Les rôles d'utilisateur et les privilèges d'accès attribués à chacun;

(c) Les exigences uniques des contrôles de sécurité;

(d) Les types d'information traités, stockés ou transmis par le système, incluant tout besoin de protection stipulé dans les lois du GC et les politiques, directives et normes concernées du SCT; et

(e) La priorité de restauration de l'information ou des services du système.

Conseils supplémentaires d'amélioration : Les exigences uniques des contrôles de sécurité du système incluent, par exemple, le chiffrement des éléments de données clés inactifs. Les besoins de protection spécifiques du système peuvent être stipulés, par exemple, dans la Loi sur la protection des renseignements personnels.

Références :

Guide de vérification – Sécurité des technologies de l'information du SCT [Référence 30].
*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

PL-3 MISE À JOUR DU PLAN DE SÉCURITÉ DES SYSTÈMES

[Annulé : intégré au contrôle PL-2].

PL-4 RÈGLES DE CONDUITE

Contrôle :

(A) L'organisation établit les règles qui décrivent les responsabilités et le comportement attendu de tous les utilisateurs concernant l'utilisation de l'information et du système et leur en facilite l'accès.

(B) L'organisation, avant de les autoriser à accéder à l'information et au système, reçoit des utilisateurs une reconnaissance écrite indiquant qu'ils ont lu et compris les règles de conduite et conviennent de s'y conformer.

Conseils supplémentaires : L'organisation prévoit des ensembles de règles différentes selon les rôles et les responsabilités des utilisateurs, par exemple, des règles pour les utilisateurs privilégiés et d'autres pour les utilisateurs généraux . Les signatures électroniques sont acceptables pour la reconnaissance des règles de conduite. Contrôle connexe : PS-6.

Améliorations du contrôle :

(1) L'organisation inclut dans les règles de conduite des restrictions explicites concernant l'utilisation des sites de réseaux sociaux, l'affichage d'information dans les sites Web commerciaux et le partage d'information avec le compte de système.

Références :

Aucune.

PL-5 ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

Contrôle :

(A) L'organisation effectue une évaluation des facteurs relatifs à la vie privée du système d'information en conformité avec la *Politique d'évaluation des facteurs relatifs à la vie privée du SCT* [Référence 25].

Conseils supplémentaires : Aucune.

Améliorations du contrôle :

Aucune.

Références :

Politique d'évaluation des facteurs relatifs à la vie privée du SCT [Référence 25].

PL-6 PLANIFICATION DES ACTIVITÉS RELATIVES À LA SÉCURITÉ

Contrôle :

(A) L'organisation planifie et coordonne les activités liées à la sécurité du système d'information avant de les appliquer afin de réduire leur incidence sur les activités organisationnelles (c.-à-d., mission, fonctions, image et réputation), les biens de l'organisation et les individus.

Conseils supplémentaires : Les activités liées à la sécurité incluent, par exemple, les évaluations de la sécurité, les vérifications, la maintenance du matériel et du logiciel de système et les tests et (ou) exercices liés au plan des mesures d'urgence. L'organisation effectue une planification et une coordination préliminaires pour les situations à la fois urgentes et non urgentes (c.-à-d., planifiées ou non urgentes et non planifiées).

Améliorations du contrôle :

Aucune.

Références :

Aucune.

4.13 FAMILLE : SÉCURITÉ DU PERSONNEL

CLASSE : OPÉRATIONNELLE

PS-1 POLITIQUE ET PROCÉDURES DE SÉCURITÉ DU PERSONNEL

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique de sécurité du personnel formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de sécurité du personnel et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de sécurité du personnel. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique de sécurité du personnel peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures de sécurité du personnel peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique de sécurité du personnel. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

PS-2 CATÉGORISATION DES POSTES

Contrôle :

(A) L'organisation catégorise tous les postes en fonction des préjudices que les individus peuvent causer en commettant des actes malveillants découlant de l'exercice des privilèges associés à leur poste.

(B) L'organisation choisit le niveau de filtrage approprié (p. ex., ERC, I, II, III) pour les titulaires des postes.

(C) L'organisation examine et révise les catégorisations des postes [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Aucune.

Améliorations du contrôle :

Aucune.

Références :

Norme sur la sécurité du personnel du SCT [Référence 10].

PS-3 ENQUÊTE DE SÉCURITÉ SUR LE PERSONNEL

Contrôle :

(A) L'organisation filtre les individus avant d'autoriser l'accès au système d'information, en conformité avec la *Norme sur la sécurité du personnel du SCT* [Référence 10].

(B) L'organisation filtre les individus de nouveau lorsque [*Affectation : liste définie par l'organisation des conditions qui exigent un nouveau filtrage et fréquence de ce filtrage, le cas échéant*].

Conseils supplémentaires : Les deux types de filtrage sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT ainsi qu'aux critères établis pour la désignation des risques associés au poste concerné. L'organisation peut définir différentes conditions et fréquences pour le nouveau filtrage des employés qui accèdent au système selon le type d'information traité, stocké ou transmis.

Améliorations du contrôle :

(1) L'organisation s'assure que chaque utilisateur d'un système d'information qui traite, stocke ou transmet de l'information classifiée possède une cote de sécurité équivalente au plus haut niveau de classification de l'information contenue dans le système.

(2) L'organisation s'assure que chaque utilisateur d'un système d'information qui traite, stocke ou transmet des types d'information classifiée cotée formellement possède la cote de sécurité requise pour tous les types d'information.

Conseils supplémentaires d'amélioration : L'information sensible cloisonnée est un exemple de type d'information qui doit être cotée formellement.

Références :

Manuel de la sécurité industrielle de TPSGC [Référence 3].
Norme sur la sécurité du personnel du SCT [Référence 10].

PS-4 CESSATION D'EMPLOI

Contrôle :

(A) L'organisation, lors de la cessation d'emploi d'un individu, met un terme à l'accès du système d'information.

(B) L'organisation, lors de la cessation d'emploi d'un individu, effectue des entrevues de fin d'emploi.

(C) L'organisation, lors de la cessation d'emploi d'un individu, retire tous les biens de l'organisation associés à la sécurité du système d'information.

(D) L'organisation, lors de la cessation d'emploi d'un individu, maintient l'accès à l'information organisationnelle et aux systèmes d'information en conformité avec la *Norme sur la sécurité du personnel du SCT* [Référence 10].

Conseils supplémentaires : Les biens associés au système d'information incluent, par exemple, les jetons matériels d'authentification, les manuels techniques d'administration du système, les clés, les cartes d'identité et les laissez-passer. Les entrevues de fin d'emploi permettent de s'assurer que les individus comprennent les contraintes de sécurité auxquelles ils doivent se soumettre à titre d'anciens employés et leurs responsabilités à l'égard de tous les biens associés au système d'information. Il peut arriver qu'il soit impossible de procéder à ces

entrevues pour certains employés (p. ex., dans le cas d'un abandon de poste, de certaines maladies et de la non-disponibilité des superviseurs). Les entrevues sont importantes dans le cas des individus qui possèdent une cote de sécurité. L'exécution de ce contrôle dans les meilleurs délais est particulièrement importante dans le cas d'employés ou d'entrepreneurs licenciés.

Améliorations du contrôle :

Aucune.

Références :

Norme sur la sécurité du personnel du SCT [Référence 10].

PS-5 TRANSFERT DE PERSONNEL

Contrôle :

(A) L'organisation examine les autorisations d'accès physique et logique aux systèmes d'information et (ou) aux installations lorsque le personnel est réaffecté ou transféré dans d'autres postes au sein de l'organisation et entreprend des [*Affectation :mesures de transfert ou de réaffectation définies par l'organisation*] dans les [*Affectation : durée définie par l'organisation conformément à la Norme sur la sécurité du personnel du SCT* [Référence 10]].

Conseils supplémentaires : Ce contrôle s'applique dans le cas où la réaffectation ou le transfert d'un employé sont permanents ou d'une durée qui justifie les mesures requises. En plus, l'organisation définit les mesures appropriées pour le type de réaffectation ou de transfert, qu'ils soient permanents ou temporaires. Ces mesures incluent, par exemple, (i) le retour et le remplacement des anciennes clés, cartes d'identité et laissez-passer, (ii) la fermeture des anciens comptes de système et l'établissement de nouveaux, (iii) la modification des autorisations d'accès aux systèmes d'information et (iv) la réinstauration de l'accès aux dossiers officiels auxquels l'employé avait accès dans le lieu de travail précédent et avec les comptes de système précédents.

Améliorations du contrôle :

Aucune.

Références :

Norme sur la sécurité du personnel du SCT [Référence 10].

PS-6 ENTENTES D'ACCÈS

Contrôle :

(A) L'organisation s'assure que les individus qui ont besoin d'accéder à l'information organisationnelle et aux systèmes d'information signent les ententes d'accès appropriées avant que l'accès ne leur soit accordé.

(B) L'organisation examine et (ou) met à jour les ententes d'accès [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires : Les ententes d'accès incluent, par exemple, les ententes de non-divulgation, les ententes d'utilisation acceptable, les règles de conduite et les ententes régissant les conflits d'intérêts. Les ententes d'accès signées incluent une attestation que l'individu a lu et compris les contraintes associées au système concerné et accepte de s'y conformer. Les signatures électroniques sont acceptables, sauf là où elles sont expressément interdites par la politique de l'organisation. Contrôle connexe : PL-4.

Améliorations du contrôle :

(1) L'organisation s'assure que l'accès à l'information visée par des mesures de protection spéciales est accordé uniquement aux individus qui :

(a) Possèdent une autorisation d'accès valable attestée par les responsabilités gouvernementales officielles qui leur ont été assignées; et

(b) Satisfont aux critères correspondants de sécurité du personnel.

Conseils supplémentaires d'amélioration : L'information visée par des mesures de protection spéciales inclut, par exemple, l'information sur la vie privée et propriétaire. Les critères de sécurité du personnel incluent, par exemple, les exigences du poste concernant la vérification des antécédents en matière de sensibilité de l'information.

(2) L'organisation s'assure que l'accès à l'information classifiée visée par des mesures de protection spéciales est accordé uniquement aux individus qui :

(a) Possèdent une autorisation d'accès valable attestée par les responsabilités gouvernementales officielles qui leur ont été assignées;

(b) Satisfont aux critères correspondants de sécurité du personnel; et

(c) Ont lu, compris et signé une entente de non-divulgation.

Conseils supplémentaires d'amélioration : L'information sensible cloisonnée est un exemple de type d'information qui doit être cotée formellement. Les critères de sécurité du personnel sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT.

Références :

Aucune.

PS-7 SÉCURITÉ DU PERSONNEL TIERS

Contrôle :

(A) L'organisation définit les exigences du contrôle de la sécurité du personnel, incluant les rôles et responsabilités des fournisseurs tiers en matière de sécurité.

(B) L'organisation documente les exigences du contrôle de la sécurité du personnel.

(C) L'organisation surveille la conformité des fournisseurs.

(AA) L'organisation s'assure d'effectuer le filtrage de sécurité des organisations et des individus du secteur privé qui ont accès à l'information et aux biens protégés et classifiés, en conformité avec la *Norme sur la sécurité du personnel du SCT* [Référence 10].

(BB) L'organisation définit explicitement la surveillance gouvernementale et les rôles et responsabilités d'utilisateur final relativement aux services de tiers, en conformité avec la *Norme de sécurité et de gestion des marchés du SCT* [Référence 26].

Conseils supplémentaires : Les fournisseurs tiers incluent, par exemple, les sociétés de services informatiques, les entrepreneurs et autres organisations qui offrent des services de développement de système d'information et de technologie de l'information, les applications imparties et la gestion des réseaux et de la sécurité. L'organisation inclut explicitement les exigences du contrôle de la sécurité du personnel dans les documents d'approvisionnement.

Améliorations du contrôle :

Aucune.

Références :

Norme sur la sécurité du personnel du SCT [Référence 10].
Norme de sécurité et de gestion des marchés du SCT [Référence 26].

PS-8 SANCTIONS IMPOSÉES AU PERSONNEL

Contrôle :

(A) L'organisation utilise un processus formel de sanctions pour le personnel qui ne se conforme pas aux politiques et procédures établies de sécurité de l'information.

Conseils supplémentaires : Le processus de sanctions est conforme aux lois du GC et aux politiques, directives et normes concernées du SCT. Le processus est décrit dans des ententes d'accès et peut être inclus dans les politiques et procédures générales sur le personnel de l'organisation. Contrôles connexes : PL-4, PS-6.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

4.14 FAMILLE : ÉVALUATION DES RISQUES

CLASSE : GESTION

RA-1 POLITIQUE ET PROCÉDURES D'ÉVALUATION DES RISQUES

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique d'évaluation des risques formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique d'évaluation des risques et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles d'évaluation des risques. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique d'évaluation des risques peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures d'évaluation des risques peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique d'évaluation des risques. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

RA-2 CATÉGORIES DE SÉCURITÉ

Contrôle :

(A) L'organisation catégorise l'information et les systèmes d'information en conformité avec les lois pertinentes du GC et les politiques, directives et normes du SCT.

(B) L'organisation documente les résultats de la catégorisation (incluant la logique correspondante) dans le plan de sécurité du système d'information.

(C) L'organisation s'assure que les décisions concernant les catégories sont examinées et approuvées par l'agent d'autorisation ou un représentant désigné.

Conseils supplémentaires : Une limite d'autorisation clairement définie est un préalable à l'établissement efficace des catégories de sécurité. Les catégories décrivent les incidences négatives potentielles sur les activités organisationnelles, les biens de l'organisation et les individus résultant de la compromission de l'information et des systèmes suite à une perte de confidentialité, d'intégrité ou de disponibilité. L'organisation accorde au

processus de catégorisation de la sécurité le statut d'activité organisationnelle à laquelle participent le dirigeant principal de l'information, l'agent principal de sécurité de l'information, les propriétaires des systèmes d'information, les propriétaires de la mission et les propriétaires et les gardiens de l'information. Lors de la catégorisation, l'organisation tient également compte des incidences négatives potentielles sur les autres organisations ainsi que des incidences négatives à l'échelle nationale. Le processus de catégorisation facilite la création d'un inventaire des ressources d'information et, de pair avec le contrôle CM-8, permet d'établir un lien avec les composantes du système d'information qui traitent, stockent et transmettent l'information. Contrôles connexes : CM-8, MP-4, SC-7.

Améliorations du contrôle :

Aucune.

Références :

Annexe 2 du Guide de gestion des risques de sécurité des systèmes d'information – Processus de mise en œuvre de la sécurité de l'information (ITSG-33) du CSTC [Référence 60].

RA-3 ÉVALUATION DES RISQUES

Contrôle :

(A) L'organisation effectue une évaluation des risques, incluant la probabilité et l'ampleur des préjudices, associés aux différents aspects du système d'information (accès non autorisé, utilisation, divulgation, interruption, modification ou destruction) et de l'information qu'il traite, stocke et transmet, en conformité avec la *norme Sécurité relative à l'organisation et l'administration du SCT* [Référence 14].

(B) L'organisation documente les résultats de l'évaluation dans [*Sélection : plan de sécurité; rapport d'évaluation des risques;[Affectation : document défini par l'organisation]*]

(C) L'organisation examine les résultats de l'évaluation [*Affectation : fréquence définie par l'organisation*].

(D) L'organisation effectue une mise à jour de l'évaluation [*Affectation : fréquence définie par l'organisation*] ou chaque fois que des changements importants sont apportés au système ou à l'environnement d'exploitation (incluant l'identification des nouvelles menaces et vulnérabilités), ou lorsque d'autres conditions sont susceptibles d'influer sur l'état de sécurité du système.

Conseils supplémentaires : Une limite d'autorisation clairement définie est un préalable à une évaluation efficace des risques. Les évaluations tiennent compte des vulnérabilités, des sources de menaces et des contrôles de sécurité prévus ou existants afin de déterminer, au plan de l'exploitation du système, le niveau de risque résiduel pour les activités et les biens de l'organisation, les individus, les autres organisations et le Canada. Elles tiennent également compte des risques que représentent les intervenants externes pour les activités organisationnelles, les biens de l'organisation ou les individus (p. ex., fournisseurs de services, entrepreneurs qui exploitent les systèmes au nom de l'organisation, individus qui accèdent aux systèmes de l'organisation, impartiteurs).

Les évaluations (formelles ou informelles) peuvent être effectuées à différents stades du cadre de gestion du risque (ITSG-33), incluant la catégorisation du système, la sélection des contrôles de sécurité, la mise en œuvre des contrôles et leur évaluation, l'autorisation des systèmes et la surveillance des contrôles. Le contrôle RA-3 est particulier; il doit être *appliqué* partiellement avant la mise en œuvre des autres contrôles afin de permettre de terminer les deux premières étapes de la gestion du risque.

Améliorations du contrôle :

Aucune.

Références :

Annexe 2 du Guide de gestion des risques de sécurité des systèmes d'information – Processus de mise en œuvre de la sécurité de l'information (ITSG-33) du CSTC [Référence 60].
Méthodologie harmonisée d'évaluation des menaces et des risques (GRC) du CSTC [Référence 4].
Norme Sécurité relative à l'organisation et l'administration du SCT [Référence 14].

RA-4 MISE À JOUR DE L'ÉVALUATION DES RISQUES

[Annulé : Intégré au contrôle RA-3].

RA-5 ANALYSE DES VULNÉRABILITÉS

Contrôle :

(A) L'organisation identifie les vulnérabilités dans le système d'information et les applications hébergées [*Affectation : fréquence définie par l'organisation et (ou) de manière aléatoire en conformité avec le processus défini par l'organisation*] et lorsque de nouvelles vulnérabilités susceptibles d'influer sur le système et (ou) les applications sont identifiées et signalées.

(B) L'organisation utilise des outils et des techniques d'analyse des vulnérabilités qui favorisent l'interopérabilité entre eux et les composantes automatisées du processus de gestion des vulnérabilités; à cette fin, elle applique des normes sur les aspects suivants :

(a) Relevé des plate-formes, des lacunes logicielles et des configurations inappropriées;

(b) Formatage de listes de vérification et de procédures de test transparentes; et

(c) Mesure des répercussions des vulnérabilités.

(C) L'organisation examine les rapports d'analyse des vulnérabilités et les résultats des évaluations des contrôles de sécurité.

(D) L'organisation corrige les vulnérabilités légitimes [*Affectation : temps de réponse définis par l'organisation*] en conformité avec son évaluation des risques.

(E) L'organisation partage l'information obtenue du processus d'analyse des vulnérabilités et des évaluations des contrôles avec tout le personnel désigné de l'organisation pour faciliter la suppression de vulnérabilités similaires (c.-à-d., faiblesses ou lacunes systémiques) dans les autres systèmes d'information.

Conseils supplémentaires : Les catégories de sécurité du système d'information permettent de définir la fréquence et le niveau d'exhaustivité des analyses des vulnérabilités. Les analyses des vulnérabilités des applications et des logiciels personnalisés peuvent exiger des techniques et des approches supplémentaires plus spécialisées (p. ex., analyseurs d'application Web, examens du code source, analyseurs de code source). Elles incluent la recherche de fonctions, ports, protocoles et services spécifiques qui ne doivent pas être accessibles aux utilisateurs ou aux dispositifs et l'identification des mécanismes de flux d'information mal configurés ou fonctionnant de façon inappropriée.

Améliorations du contrôle :

(1) L'organisation utilise des outils d'analyse des vulnérabilités capables de tenir facilement à jour la liste des vulnérabilités relevées.

(2) L'organisation met à jour la liste des vulnérabilités relevées [*Affectation : fréquence définie par l'organisation*] ou lorsque de nouvelles vulnérabilités sont identifiées et signalées.

(3) L'organisation utilise des procédures d'analyse des vulnérabilités capables de rendre compte de l'ampleur et de la profondeur de la couverture (c.-à-d., composantes analysées et vulnérabilités vérifiées).

(4) L'organisation tente d'établir la nature de l'information que des adversaires peuvent découvrir à propos du système.

(5) L'organisation prévoit une autorisation d'accès privilégié aux [*Affectation : composantes de système définies par l'organisation*] pour certaines activités d'analyse des vulnérabilités afin de permettre une analyse plus poussée.

(6) L'organisation utilise des mécanismes automatisés pour comparer chronologiquement les résultats des analyses et déterminer les tendances en matière de vulnérabilités.

(7) L'organisation utilise des mécanismes automatisés [*Affectation : fréquence définie par l'organisation*] pour détecter la présence de logiciels non autorisés dans les systèmes d'information et en informer les agents désignés de l'organisation.

(8) L'organisation examine les journaux de vérification historiques pour déterminer si une vulnérabilité identifiée dans le système a déjà été exploitée.

(9) L'organisation fait appel à une équipe ou un agent de pénétration indépendant pour :

(a) Analyser les vulnérabilités du système; et

(b) Effectuer des tests de pénétration fondés sur l'analyse pour déterminer la mesure dans laquelle les vulnérabilités identifiées peuvent être exploitées.

Conseils supplémentaires d'amélioration : Une méthode standard de test de pénétration inclut (i) l'analyse préalable de l'information basée sur une connaissance détaillée du système cible, (ii) l'identification préalable des vulnérabilités potentielles basée sur l'analyse et (iii) l'exécution des tests conçus pour déterminer la mesure dans laquelle les vulnérabilités identifiées peuvent être exploitées. Toutes les parties doivent convenir des règles d'engagement détaillées avant le commencement de tout scénario de test de pénétration.

Références :

Aucune.

4.15 FAMILLE : ACQUISITION DES SYSTÈMES ET DES SERVICES

CLASSE : GESTION

SA-1 POLITIQUE ET PROCÉDURES D'ACQUISITION DES SYSTÈMES ET DES SERVICES

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique d'acquisition des systèmes et des services formelle et documentée qui inclut des éléments liés à la sécurité de l'information et définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique d'acquisition des systèmes et des services et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles d'acquisition des systèmes et des services. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique d'acquisition des systèmes et des services peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures d'acquisition des systèmes et des services peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique d'acquisition des systèmes et des services. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

SA-2 AFFECTATION DES RESSOURCES

Contrôle :

(A) L'organisation identifie les exigences en matière de contrôle de sécurité de l'information pour la planification du processus lié à la mission et aux opérations.

(B) L'organisation détermine, documente et affecte les ressources nécessaires pour protéger le processus de contrôle de la planification des immobilisations et des investissements du système d'information.

(C) L'organisation établit un poste distinct pour la sécurité de l'information dans la documentation de programmation et de budgétisation de l'organisation.

Conseils supplémentaires : Contrôles connexes : PM-3, PM-11.

Améliorations du contrôle :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

Références :

Aucune.

SA-3 SOUTIEN DU CYCLE DE VIE

Contrôle :

(A) L'organisation gère le système d'information en utilisant une méthodologie de cycle de développement des systèmes qui inclut les aspects liés à la sécurité de l'information.

(B) L'organisation définit et documente les rôles et responsabilités associés à la sécurité de l'information à tous les stades du cycle de développement des systèmes.

(C) L'organisation identifie les personnes auxquelles sont attribués des rôles et des responsabilités associés à la sécurité de l'information.

Conseils supplémentaires : Contrôle connexe : PM-7.

Améliorations du contrôle :

Aucune.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

SA-4 ACQUISITIONS

Contrôle :

(A) L'organisation inclut, explicitement ou en référence, dans les contrats d'acquisition de systèmes des exigences et (ou) des spécifications fonctionnelles de sécurité basées sur une évaluation des risques, en conformité avec les lois du GC et les politiques, directives et normes concernées du SCT.

(B) L'organisation inclut, explicitement ou en référence, dans les contrats d'acquisition de systèmes de la documentation sur la sécurité ainsi que des exigences et (ou) des spécifications fonctionnelles de sécurité basées sur une évaluation des risques, en conformité avec la *Norme de sécurité et de gestion des marchés du SCT* [Référence 26].

(C) L'organisation inclut, explicitement ou en référence, dans les contrats d'acquisition de systèmes les exigences et (ou) les spécifications de développement et d'évaluation basées sur une évaluation des risques, en conformité avec les lois du GC et les politiques, directives et normes concernées du SCT.

Conseils supplémentaires : Les documents d'acquisition des systèmes, des composantes et des services incluent, explicitement ou en référence, des exigences sur les contrôles de sécurité qui décrivent (i) les capacités de sécurité requises (c.-à-d., les exigences de sécurité et, le cas échéant, des contrôles de sécurité spécifiques et autres exigences organisationnelles et gouvernementales), (ii) les processus de conception et de développement requis, (iii) les procédures de test et d'évaluation requises et (iv) la documentation pertinente. Ces exigences permettent la mise à jour des contrôles de sécurité au fur et à mesure de l'identification de nouvelles menaces et (ou) vulnérabilités et de l'application des nouvelles technologies. Les documents d'acquisition incluent également des exigences concernant la documentation appropriée des systèmes. Cette documentation inclut des

directives sur l'utilisation et l'administration des systèmes ainsi que de l'information concernant l'application des contrôles de sécurité. Le niveau de détail requis de la documentation est dicté par les catégories de sécurité du système. La documentation inclut également les paramètres de configuration de la sécurité et des directives sur la mise en œuvre de la sécurité.

Améliorations du contrôle :

(1) L'organisation exige dans les documents d'acquisition que les fournisseurs et (ou) entrepreneurs décrivent, d'une manière suffisamment détaillée pour en permettre l'analyse et les tests, les propriétés fonctionnelles des contrôles de sécurité utilisés dans le système et ses composantes ou services.

(2) L'organisation exige dans les documents d'acquisition que les fournisseurs et (ou) entrepreneurs décrivent, d'une manière suffisamment détaillée pour en permettre l'analyse et les tests, la conception et la mise en œuvre des contrôles de sécurité utilisés dans le système et ses composantes ou services (incluant les interfaces fonctionnelles des composantes de contrôle).

(3) L'organisation exige des fournisseurs et (ou) fabricants de logiciel qu'ils prouvent que leurs processus de développement de logiciel utilisent des méthodes d'ingénierie de logiciel et de sécurité, des processus de contrôle de la qualité et des techniques de validation à la fine pointe de la technologie afin de réduire les lacunes ou les défectuosités du logiciel.

(4) L'organisation s'assure que chaque composante de système acquise soit explicitement assignée à un système et que le propriétaire du système atteste de cette assignation.

(5) L'organisation exige dans les documents d'acquisition que la configuration des composantes de système livrées soient sécurisée et documentée et que cette configuration soit celle utilisée pour toutes les réinstallations ou les mises à niveau de logiciel.

(6) L'organisation :

(a) Utilise seulement des produits de TI sécurisés gouvernementaux (GOTS) ou commerciaux (COTS) standard comme solution approuvée par le CSTC afin de protéger l'information classifiée transmise dans des réseaux dont le niveau de classification est inférieur à celui de l'information; et

(b) S'assure que ces produits ont été évalués et (ou) validés par le CSTC ou en conformité avec des procédures approuvées par le Centre.

Conseils supplémentaires d'amélioration : Les produits de TI sécurisés COTS utilisés pour protéger l'information classifiée par des moyens cryptographiques doivent utiliser une méthode de gestion des clés approuvée par le CSTC. La cryptographie doit être conforme aux exigences du contrôle de sécurité SC-13 et à celles énoncées dans le document *Guide to Interconnecting Security Domains (ITSG-32) du CSTC* [Référence 23].

(7) L'organisation :

(a) Limite l'utilisation des produits de TI commerciaux à ceux qui ont été évalués avec succès par le CSTC lorsqu'une telle évaluation existe; et

(b) Exige que le module cryptographique, qu'utilise un produit de TI commercial pour appliquer sa politique de sécurité, soit conforme aux exigences du contrôle SC-13.

Conseils supplémentaires d'amélioration : Contrôle connexe : SC-13.

Références :

Norme de sécurité et de gestion des marchés du SCT [Référence 26].
Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés (ITSA-11D) du CSTC [Référence 9].
Guide to Interconnecting Security Domains (ITSG-32) du CSTC [Référence 23].
Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B (ITSB-40) du CSTC [Référence 29].

SA-5 DOCUMENTATION DES SYSTÈMES D'INFORMATION

Contrôle :

(A) L'organisation obtient, protège de manière adéquate et transmet au personnel autorisé une documentation d'administrateur de système qui décrit :

(a) La configuration, l'installation et l'exploitation sécuritaires du système d'information;

(b) L'utilisation et la maintenance efficace des fonctions de sécurité; et

(c) Les vulnérabilités connues associées à la configuration et l'utilisation des fonctions administratives (c.-à-d., privilégiées).

(B) L'organisation obtient, protège de manière adéquate et transmet au personnel autorisé une documentation d'utilisateur de système qui décrit :

(a) Les fonctions de sécurité accessibles à l'utilisateur et la façon de les utiliser efficacement;

(b) Les méthodes d'interaction de l'utilisateur avec le système d'information qui lui permettent de l'utiliser de manière plus sécuritaire; et

(c) Les responsabilités de l'utilisateur concernant la protection de l'information et du système d'information.

(C) L'organisation documente les tentatives d'obtenir une documentation de système qui n'existe pas ou qui n'est pas disponible.

Conseils supplémentaires : L'incapacité pour l'organisation d'obtenir la documentation de système requise peut être due, par exemple, à l'âge du système et (ou) à l'absence de soutien du fournisseur et (ou) de l'entrepreneur. Dans ces situations, l'organisation devra peut-être recréer une documentation sélective si elle est essentielle à la mise en œuvre et (ou) à l'exploitation efficaces des contrôles de sécurité.

Améliorations du contrôle :

(1) L'organisation obtient, protège de manière adéquate et transmet au personnel autorisé la documentation du fournisseur et (ou) du fabricant qui décrit, d'une manière suffisamment détaillée pour en permettre l'analyse et les tests, les propriétés fonctionnelles des contrôles de sécurité utilisés dans le système.

(2) L'organisation obtient, protège de manière adéquate et transmet au personnel autorisé la documentation du fournisseur et (ou) du fabricant qui décrit, d'une manière suffisamment détaillée pour en permettre l'analyse et les tests, les interfaces de sécurité externes du système.

(3) L'organisation obtient, protège de manière adéquate et transmet au personnel autorisé la documentation du fournisseur et (ou) du fabricant qui décrit, d'une manière suffisamment détaillée pour en permettre l'analyse et les tests, la conception de haut niveau du système (sous-systèmes et détails d'application des contrôles de sécurité).

Conseils supplémentaires d'amélioration : Un système d'information peut être partitionné en plusieurs sous-systèmes.

(4) L'organisation obtient, protège de manière adéquate et transmet au personnel autorisé la documentation du fournisseur et (ou) du fabricant qui décrit, d'une manière suffisamment détaillée pour en permettre l'analyse et les tests, la conception de bas niveau du système (modules et détails d'application des contrôles de sécurité).

Conseils supplémentaires d'amélioration : Chaque sous-système d'un système d'information peut inclure un ou plusieurs modules.

(5) L'organisation obtient, protège de manière adéquate et transmet au personnel autorisé le code source du système pour en permettre l'analyse et les tests.

Références :

Aucune.

SA-6 RESTRICTIONS RELATIVE À L'UTILISATION DU LOGICIEL

Contrôle :

(A) L'organisation utilise le logiciel et la documentation correspondante en conformité avec les ententes contractuelles et les lois sur le droit d'auteur.

(B) L'organisation utilise pour le logiciel et la documentation correspondante des systèmes de suivi protégés par des licences qui limitent la copie et la diffusion du produit.

(C) L'organisation contrôle et documente l'utilisation de la technologie de partage de fichiers pair à pair pour s'assurer qu'elle n'est pas utilisée à des fins d'affichage et de diffusion non autorisées ou de reproduction en contravention du droit d'auteur.

Conseils supplémentaires : Les systèmes de suivi peuvent inclure, par exemple, de simples feuilles de calcul ou des applications entièrement automatisées, selon les besoins de l'organisation.

Améliorations du contrôle :

(1) L'organisation :

(a) Interdit l'utilisation de code binaire ou exécutable en provenance de sources qui n'offrent pas de garantie ou qui offrent une garantie limitée sans fournir le code source; et

(b) Permet de contourner la restriction qui précède seulement dans situations urgentes liées à la mission ou aux besoins opérationnels et en l'absence de solution de secours; le responsable des autorisations doit alors donner son consentement exprès écrit.

Conseils supplémentaires d'amélioration : Les produits logiciels en provenance de sources qui n'offrent pas de garantie, ou qui offrent une garantie limitée sans fournir le code source, sont évalués au plan de leurs répercussions potentielles sur la sécurité. Ces types de produits sont effectivement difficiles ou impossibles à analyser, réparer ou développer puisque l'organisation n'a pas accès au code source original et qu'aucun propriétaire n'est en mesure d'effectuer ces réparations au nom de l'organisation.

Références :

Aucune.

SA-7 LOGICIEL INSTALLÉ PAR L'UTILISATEUR

Contrôle :

(A) L'organisation applique des règles explicites concernant l'installation de logiciel par les utilisateurs.

Conseils supplémentaires : Si on leur accorde les privilèges nécessaires, les utilisateurs peuvent installer le logiciel. L'organisation identifie les types d'installation de logiciel permis (p. ex., application des mises à jour et des rustines de sécurité au logiciel existant) et les types d'installation interdits (p. ex., logiciel dont on ignore ou soupçonne qu'ils sont potentiellement malveillants). Contrôle connexe : CM-2.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SA-8 PRINCIPES D'INGÉNIERIE DE LA SÉCURITÉ

Contrôle :

(A) L'organisation applique les principes d'ingénierie de la sécurité aux spécifications, à la conception, au développement, à la mise en œuvre et à la modification des systèmes d'information.

Conseils supplémentaires : L'application des principes d'ingénierie de la sécurité vise principalement le développement des nouveaux systèmes, ou les systèmes qui font l'objet de mises à niveau majeures, et est intégrée au cycle de développement des systèmes. Dans le cas des systèmes existants, l'organisation applique dans la mesure du possible les principes aux mises à niveau et aux modifications des systèmes en tenant compte de l'état actuel de leur matériel, logiciel et micrologiciel. Les exemples de principes d'ingénierie de la sécurité incluent, entre autres, (i) le développement de protections en couches; (ii) l'établissement de politiques, d'architectures et de contrôles de sécurité sains comme base de la conception, (iii) l'intégration de la sécurité au cycle de développement des systèmes, (iv) la délimitation des périmètres de sécurité physique et logique, (v) la formation appropriée des développeurs et des intégrateurs pour leur permettre de créer du logiciel sécurisé, (vi) la personnalisation des contrôles de sécurité en fonction des besoins organisationnels et opérationnels et (vii) la réduction des risques à des niveaux acceptables pour permettre des décisions éclairées en matière de gestion du risque.

Améliorations du contrôle :

(100) L'organisation recoure à des techniciens brevetés et agréés en sécurité qui assument la responsabilité des spécifications, de la conception, du développement et de la mise en œuvre de solutions de sécurité.

Références :

Aucune.

SA-9 SERVICES DE SYSTÈME D'INFORMATION EXTERNES

Contrôle :

(A) L'organisation exige des fournisseurs de services de système d'information externes qu'ils respectent ses exigences en matière de contrôle de sécurité de l'information et utilisent des contrôles appropriés en conformité avec la *Norme de sécurité et de gestion des marchés du SCT* [Référence 26].

(B) L'organisation définit et documente la surveillance gouvernementale et les rôles et responsabilités des utilisateurs pour ce qui touche les services de système externes.

(C) L'organisation surveille la mesure dans laquelle les fournisseurs de services externes se conforment aux contrôles de sécurité.

Conseils supplémentaires : Un service de système externe est un service qui échappe aux limites d'autorisation du système d'information de l'organisation (c.-à-d., service utilisé par le système sans en faire partie). Les relations avec les fournisseurs de services externes prennent différentes formes, par exemple, coentreprises, partenariats d'affaires, accords d'impartition (c.-à-d., contrats, ententes interorganismes, ententes liées aux secteurs d'activité), accords de licence et (ou) échanges de chaîne d'approvisionnement. L'agent d'autorisation demeure responsable d'atténuer de manière adéquate les risques liés à l'utilisation des services externes. Ces agents exigent l'établissement d'une chaîne de confiance appropriée avec les fournisseurs de services externes lorsque vient le temps de traiter des nombreux aspects liés à la sécurité de l'information. Dans le cas des services externes, la chaîne de confiance exige que l'organisation crée et maintienne un niveau de confiance en la capacité de chaque fournisseur, qui participe à une relation client-fournisseur potentiellement complexe, d'assurer une protection adéquate des services rendus. La portée et la nature de la chaîne varient en fonction de la relation qui existe entre l'organisation et le fournisseur externe. Lorsqu'il est impossible d'établir un niveau de confiance

suffisant à l'égard des services externes et (ou) des fournisseurs de services, l'organisation recoure à des contrôles de sécurité compensatoires ou accepte que le niveau de risque soit plus élevé. La documentation des services externes inclut les rôles et responsabilités du gouvernement, du fournisseur de services et de l'utilisateur final en matière de sécurité, ainsi que toute entente de niveau de service pertinente. Les ententes définissent les attentes de rendement pour chaque contrôle de sécurité obligatoire, décrivent les produits mesurables et identifient les exigences relatives aux solutions et aux interventions pour chaque situation de non conformité relevée.

Améliorations du contrôle :

(1) L'organisation :

(a) Effectue une évaluation des risques avant l'acquisition ou l'impartition des services spécialisés de sécurité de l'information; et

(b) S'assure que l'acquisition ou l'impartition de ces services est approuvée par [*Affectation : cadre supérieur désigné par l'organisation*].

Conseils supplémentaires d'amélioration : Les services spécialisés de sécurité de l'information incluent, par exemple, la surveillance et l'analyse des incidents et les interventions correspondantes, et l'exploitation des dispositifs de sécurité tels les pare-feu, ou les services de gestion des clés.

Références :

Norme de sécurité et de gestion des marchés du SCT [Référence 26].

SA-10 GESTION DE LA CONFIGURATION PAR LES DÉVELOPPEURS

Contrôle :

(A) L'organisation exige que les développeurs et (ou) les intégrateurs de système gèrent la configuration durant la conception, le développement, la mise en œuvre et l'exploitation du système.

(B) L'organisation exige que les développeurs et (ou) les intégrateurs de système gèrent et contrôlent les changements apportés au système.

(C) L'organisation exige que les développeurs et (ou) les intégrateurs de système mettent en œuvre uniquement les changements qu'elle approuve.

(D) L'organisation exige que les développeurs et (ou) les intégrateurs de système documentent les changements approuvés apportés au système.

(E) L'organisation exige que les développeurs et (ou) les intégrateurs de système assurent le suivi des lacunes de sécurité et de leurs solutions.

Conseils supplémentaires : Contrôles connexes : CM-3, CM-4, CM-9.

Améliorations du contrôle :

(1) L'organisation exige que les développeurs et (ou) les intégrateurs de système effectuent un contrôle d'intégrité du logiciel pour faciliter la vérification de son intégrité après sa livraison.

(2) L'organisation prévoit un processus de secours pour ses employés en l'absence d'une équipe de développeurs et (ou) d'intégrateurs spécialisés en gestion des configurations.

Conseils supplémentaires d'amélioration : Le processus de gestion de la configuration mise sur des employés clés de l'organisation pour examiner et approuver les changements proposés et sur du personnel de sécurité pour effectuer des analyses des incidences des changements avant leur mise en œuvre.

Références :

Aucune.

SA-11 TESTS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS

Contrôle :

(A) L'organisation exige que les développeurs et (ou) les intégrateurs de système, en consultation avec le personnel chargé de la sécurité (incluant les techniciens en sécurité), créent et mettent en œuvre un plan de test et d'évaluation de la sécurité.

(B) L'organisation exige que les développeurs et (ou) les intégrateurs de système, en consultation avec le personnel chargé de la sécurité (incluant les techniciens en sécurité), mettent en œuvre un processus vérifiable de correction des problèmes pour solutionner les faiblesses et les lacunes relevées durant le processus de test et d'évaluation de la sécurité.

(C) L'organisation exige que les développeurs et (ou) les intégrateurs de système, en consultation avec le personnel chargé de la sécurité (incluant les techniciens en sécurité), documentent les résultats des processus de test et d'évaluation de la sécurité et de correction des lacunes.

Améliorations du contrôle :

(1) L'organisation exige que les développeurs et (ou) les intégrateurs de système utilisent des outils d'analyse de code pour identifier les lacunes logicielles communes et documentent les résultats de l'analyse.

(2) L'organisation exige que les développeurs et (ou) les intégrateurs de système effectuent une analyse des vulnérabilités pour documenter les vulnérabilités, leur potentiel d'exploitation et l'atténuation du risques.

(3) L'organisation exige que les développeurs et (ou) les intégrateurs de système créent un plan de test et d'évaluation de la sécurité et le mettent en œuvre sous la surveillance d'un agent de vérification et de validation indépendant.

Références :

Aucune.

SA-12 PROTECTION DE LA CHAÎNE D'APPROVISIONNEMENT

Contrôle :

(A) L'organisation protège la chaîne d'approvisionnement contre les menaces en utilisant [*Affectation : liste définie par l'organisation des mesures de protection contre les menaces liées à la chaîne d'approvisionnement*] dans le cadre d'une stratégie détaillée de défense en profondeur de la sécurité de l'information.

Conseils supplémentaires : La politique et les procédures d'acquisition des systèmes et des services sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Une approche de défense en profondeur aide à protéger les systèmes (incluant les produits de TI qui les composent) pendant tout le CDS (c.-à-d., conception et développement, fabrication, emballage, assemblage, distribution, intégration au système, exploitation, maintenance et mise hors service). Cette protection est assurée par l'identification, la gestion et l'élimination des vulnérabilités propres à chaque phase du cycle de vie et par le recours à des stratégies complémentaires mutuellement renforcées pour atténuer le risque.

Améliorations du contrôle :

(1) L'organisation achète lors de l'acquisition initiale toutes les composantes et les pièces de rechange de système dont elle prévoit avoir besoin.

Conseils supplémentaires d'amélioration : L'accumulation de composantes et de pièces de rechange permet d'éviter le besoin de s'approvisionner ultérieurement dans des marchés de revente ou secondaires moins fiables.

(2) L'organisation effectue un examen préalable des fournisseurs avant de conclure des marchés pour l'acquisition de matériel, de logiciel, de micrologiciel ou de services de système d'information.

Conseils supplémentaires d'amélioration : Utiliser des processus de sécurité appropriés pour le développement et la fabrication des composantes ou des produits de système d'information.

(3) L'organisation utilise des procédures fiables d'entreposage et d'expédition pour les systèmes, les composantes et les produits de TI.

Conseils supplémentaires d'amélioration : Les procédures d'entreposage et d'expédition fiables permettent de réduire les possibilités d'activités subversives ou d'interception durant le transit des biens. Les exemples de techniques de soutien de ces procédures incluent l'utilisation de radio-balises géographiques qui permettent de détecter les détournements et les retards de livraison. Contrôle connexe : PE-16.

(4) L'organisation utilise un ensemble varié de fournisseurs de systèmes, de composantes, de produits et de services.

Conseils supplémentaires d'amélioration : La diversification des fournisseurs vise à limiter tout préjudice potentiel lié à un fournisseur particulier de la chaîne d'approvisionnement et, ainsi, à rendre plus difficiles les activités illégales des adversaires.

(5) L'organisation utilise des configurations standard pour les systèmes, les composantes et les produits de TI.

Conseils supplémentaires d'amélioration : En évitant d'acheter des configurations personnalisées de système, de composante et de produit de TI, l'organisation réduit la possibilité d'acquérir des systèmes et des produits altérés par des manipulations de la chaîne d'approvisionnement.

(6) L'organisation réduit la période entre la décision d'acheter et la livraison des systèmes, des composantes et des produits de TI.

Conseils supplémentaires d'amélioration : En réduisant cette période, l'organisation limite les occasions pour un adversaire d'altérer le système, la composante ou le produit achetés.

(7) L'organisation applique une analyse et des tests de pénétration indépendants aux systèmes, aux composantes et aux produits de TI livrés.

Références :

Aucune.

SA-13 ROBUSTESSE (FIABILITÉ)

Contrôle :

(A) L'organisation exige du système qu'il réponde aux exigences du [*Affectation : niveau de robustesse défini par l'organisation*].

Conseils supplémentaires : Les conseils supplémentaires concernant ce contrôle seront fournis dans une prochaine version de ce document et dans des documents de conseils supplémentaires. Contrôles connexes : RA-2, SA-4, SA-8, SC-3.

Améliorations du contrôle :

Aucune.

Références :

Annexe 2 du Guide de gestion des risques de sécurité des systèmes d'information – Processus de mise en œuvre de la sécurité de l'information (ITSG-33) du CSTC [Référence 60].

SA-14 COMPOSANTES DE SYSTÈME D'INFORMATION ESSENTIELLES

Contrôle :

(A) L'organisation détermine [*Affectation : liste définie par l'organisation des composantes essentielles de système qui requièrent une nouvelle mise en œuvre*].

(B) L'organisation procède à une nouvelle mise en œuvre de ces composantes de système ou en développe des versions personnalisées.

Conseils supplémentaires : L'hypothèse sous-jacente est la suivante : la liste des produits de TI préparée par l'organisation n'est plus fiable en raison des menaces liées à la chaîne d'approvisionnement que l'organisation juge inacceptables. L'organisation procède à une nouvelle mise en œuvre des composantes ou en développe des versions personnalisées qui répondent à des exigences d'assurance élevées. Contrôles connexes : SA-12, SA-13.

Améliorations du contrôle :

(1) L'organisation :

(a) Identifie les composantes de système dont les autres sources d'approvisionnement ne sont pas viables; et

(b) Utilise [*Affectation : mesures définies par l'organisation*] pour s'assurer que les contrôles de sécurité critiques des composantes ne sont pas compromises.

Conseils supplémentaires d'amélioration : Les mesures que l'organisation envisage d'appliquer incluent, par exemple, une vérification accrue, des restrictions d'accès au code source et aux utilitaires de système et la protection contre la suppression des fichiers système et d'application.

Références :

Aucune.

4.16 FAMILLE : PROTECTION DES SYSTÈMES ET DES COMMUNICATIONS

CLASSE : TECHNIQUE

SC-1 POLITIQUE ET PROCÉDURES DE PROTECTION DES SYSTÈMES ET DES COMMUNICATIONS

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique de protection des systèmes et des communications formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de protection des systèmes et des communications et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de protection des systèmes et des communications. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique de protection des systèmes et des communications peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures de protection des systèmes et des communications peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique de protection des systèmes et des communications. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

SC-2 PARTITIONNEMENT DES APPLICATIONS

Contrôle :

(A) Le système d'information isole les fonctions d'utilisateur (incluant les services d'interface) de la fonctionnalité de gestion.

Conseils supplémentaires : La fonctionnalité de gestion inclut, par exemple, les fonctions nécessaires à l'administration des bases de données, des composantes réseau, des postes de travail ou des serveurs, et exige normalement un accès d'utilisateur privilégié. La séparation des fonctions d'utilisateur et de la fonctionnalité de gestion est soit physique, soit logique; elle est assurée par l'utilisation d'ordinateurs différents, d'unités centrales de traitement et d'instances du système d'exploitation différentes, d'adresses réseau différentes, ou de toute combinaison de ces méthodes, ou d'autres méthodes jugées appropriées. Les interfaces administratives Web, qui utilisent des méthodes d'authentification distinctes pour les utilisateurs de ressources d'autres systèmes, sont un

exemple de ce type de séparation, qui peut inclure la séparation de l'interface administrative d'un domaine différent par l'ajout de contrôles d'accès supplémentaires.

Améliorations du contrôle :

(1) Le système empêche l'utilisation de fonctions de gestion dans une interface prévue pour des utilisateurs généraux (non privilégiés).

Conseils supplémentaires d'amélioration : Le but de cette amélioration de contrôle est de veiller à ce qu'aucune option d'administration ne soit accessible aux utilisateurs généraux (incluant l'interdiction de recourir aux options grisées normalement utilisées pour empêcher l'accès à ce type d'information). Par exemple, les options d'administration ne doivent pas s'afficher tant que l'utilisateur n'a pas établi, de manière appropriée, de session donnant droit à des privilèges d'administrateur.

Références :

Aucune.

SC-3 ISOLATION DES FONCTIONS DE SÉCURITÉ

Contrôle :

(A) Le système d'information isole les fonctions de sécurité des autres fonctions.

Conseils supplémentaires : Le système isole les fonctions de sécurité des autres fonctions au moyen d'un périmètre d'isolation (défini par des partitions et des domaines) qui contrôle l'accès et protège l'intégrité du matériel, du logiciel et du micrologiciel qui accomplissent les fonctions de sécurité. Le système maintient un domaine d'exécution distinct (p. ex., espace d'adresse) pour chaque processus exécuté. Contrôle connexe : SA-13.

Améliorations du contrôle :

(1) Le système recoure à des mécanismes sous-jacents de séparation du matériel pour faciliter l'isolation des fonctions de sécurité.

(2) Le système isole, à la fois des autres fonctions de sécurité et des fonctions non liées à la sécurité, les fonctions de sécurité liées au contrôle d'accès et au flux d'information.

(3) L'organisation recoure à un périmètre d'isolation pour réduire le nombre de fonctions non liées à la sécurité qui partagent le périmètre des fonctions de sécurité.

Conseils supplémentaires d'amélioration : Les fonctions non liées à la sécurité qui occupent le périmètre d'isolation sont considérées pertinentes pour la sécurité.

(4) L'organisation applique les fonctions de sécurité sous forme de modules essentiellement indépendants qui évitent toute interaction inutile entre eux.

(5) L'organisation applique les fonctions de sécurité dans une structure en couches qui permet de réduire les interactions entre les couches de la conception et d'éviter que les couches inférieures soient assujetties au bon fonctionnement des couches supérieures ou de leurs fonctions.

Références :

Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22) du CSTC [Référence 42].
Isolation d'un serveur d'entreprise Blackberry dans un environnement Microsoft Exchange (ITSG-23) du CSTC [Référence 43].
Établissement des zones de sécurité dans un réseau – Considérations en matière de positionnement des services au sein de zones spécifiques (ITSG-38) du CSTC [Référence 44].

SC-4 INFORMATION CONTENUE DANS LES RESSOURCES PARTAGÉES

Contrôle :

(A) Le système d'information empêche tout transfert d'information non autorisé et involontaire découlant du partage des ressources du système.

Conseils supplémentaires : Le but de ce contrôle est d'empêcher l'information (incluant ses représentations chiffrées) produite par les opérations effectuées par un utilisateur ou un rôle précédent (ou un processus exécuté en leur nom) d'être transmise à un utilisateur ou un rôle (ou processus) actuel qui accède à une ressource partagée (p. ex., registres, mémoire principale, mémoire secondaire) après qu'elle a été récupérée par le système. Le contrôle de l'information contenue dans les ressources partagées est également appelé réutilisation d'un objet. Ce contrôle ne s'applique pas (i) aux fragments d'information qui désignent les représentations résiduelles de données initialement effacées ou supprimées, (ii) aux canaux cachés dans lesquels les ressources partagées sont manipulées pour restreindre les violations de flux d'information, ou (iii) aux composantes de système associées à un seul utilisateur ou rôle.

Améliorations du contrôle :

(1) Le système ne partage pas les ressources utilisées dans les interfaces avec les systèmes fonctionnant à des niveaux de sécurité différents.

Conseils supplémentaires d'amélioration : Les ressources partagées incluent, par exemple, la mémoire, les files d'entrée-sortie et les cartes d'interface réseau.

Références :

Aucune.

SC-5 PROTECTION CONTRE LES DÉNIS DE SERVICE

Contrôle :

(A) Le système d'information protège contre les types d'attaques par déni de service suivants ou en limite les effets : [*Affectation : liste définie par l'organisation des types d'attaques par déni de service ou renvoi à la source de la liste actuelle*].

Conseils supplémentaires : Il existe une variété de technologies qui limitent ou, dans certains cas, éliminent les effets des attaques par déni de service. Par exemple, les mécanismes de protection des frontières peuvent filtrer certain types de paquets pour empêcher les dispositifs du réseau interne d'une organisation d'être directement visés par des attaques par déni de service. L'utilisation d'une capacité et d'une largeur de bande accrues, combinée à la redondance des services, peut réduire la sensibilité à certaines attaques par déni de service. Contrôle connexe : SC-7.

Améliorations du contrôle :

(1) Le système limite la capacité des utilisateurs de lancer des attaques par déni de service contre d'autres systèmes ou réseaux.

(2) Le système gère l'excédent de capacité et de largeur de bande, ou de toute autre capacité de redondance, afin de limiter les effets d'attaques par déni de service de types inondation d'information.

Références :

Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22) du CSTC [Référence 42].

SC-6 PRIORITÉ DES RESSOURCES

Contrôle :

(A) Le système d'information limite l'utilisation des ressources selon peur priorité.

Conseils supplémentaires : Le respect de la priorité des ressources permet d'éviter qu'un processus de priorité inférieure empêche le système d'exécuter un processus de priorité supérieure. Ce contrôle ne s'applique pas aux composantes de système associées à un seul utilisateur ou rôle.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-7 PROTECTION DES FRONTIÈRES

Contrôle :

(A) Le système d'information surveille et contrôle les communications à sa frontière externe et à ses principales frontières internes.

(B) Le système d'information se connecte aux réseaux ou aux systèmes externes seulement par des interfaces gérées dotées de mécanismes de protection des frontières répartis en conformité avec les spécifications de l'architecture de sécurité de l'organisation.

Conseils supplémentaires : Restreindre le trafic Web externe aux seuls serveurs Web organisationnels en utilisant des interfaces gérées et interdire tout trafic externe qui semble mystifier une adresse interne en adresse source sont des exemples de restriction et d'interdiction de communications. Les interfaces gérées qui recourent à des dispositifs de protection des frontières incluent, par exemple, les mandataires, les passerelles, les routeurs, les pare-feu, les gardes de sécurité ou les tunnels chiffrés disposés en architecture de sécurité de manière efficace (p. ex., routeurs qui protègent des pare-feu et passerelles d'application hébergées dans un sous-réseau protégé appelé communément zone démilitarisée, ou DMZ).

L'organisation tient compte de la nature intrinsèquement partagée des services commerciaux de télécommunications lors de la mise en œuvre des contrôles de sécurité associés à leur utilisation. Ces services s'appuient habituellement sur des composantes réseau et des systèmes de gestion intégrés partagés par tous les clients commerciaux connectés et peuvent inclure des lignes d'accès et autres éléments de service fournis par des tiers. Ces services de transmission interconnectés peuvent donc représenter des sources de risque supplémentaire malgré les dispositions du contrat en matière de sécurité. Dans de telles situations, soit l'organisation applique des contrôles de sécurité compensatoires, soit elle accepte explicitement les risques additionnels. Contrôles connexes : AC-4, IR-4, SC-5.

Améliorations du contrôle :

(1) L'organisation attribue physiquement les composantes des systèmes accessibles au public pour séparer les sous-réseaux par des interfaces de réseau physique distinctes.

Conseils supplémentaires d'amélioration : Les composantes des systèmes accessibles au public incluent, par exemple, les serveurs Web publics.

(2) Le système empêche tout accès public aux réseaux internes de l'organisation sauf dans le cas où l'accès est négocié de manière appropriée par des interfaces gérées dotées de dispositifs de protection des frontières.

(3) L'organisation limite le nombre de points d'accès au système afin d'exercer une meilleure surveillance des communications entrantes et sortantes et du trafic réseau.

Conseils supplémentaires d'amélioration : L'initiative Consolidation des points d'accès à Internet du SCT est un exemple de restriction du nombre de points d'accès réseau gérés.

(4) L'organisation :

(a) Applique une interface gérée à chaque service de télécommunications externe;

(b) Établit une politique de flux de trafic pour chaque interface gérée;

(c) Utilise des contrôles de sécurité au besoin pour protéger la confidentialité et l'intégrité de l'information transmise;

(d) Documente chaque exception à la politique de flux de trafic; elle indique l'exigence (de la mission et (ou) de l'activité opérationnelle) à l'origine de l'exception ainsi que sa durée;

(e) Examine les exceptions à la politique de flux de trafic [*Affectation : fréquence définie par l'organisation*]; et

(f) Supprime les exceptions à la politique de flux de trafic qui ne sont plus justifiées par une exigence de mission ou opérationnelle explicite.

(5) Le système, au niveau des interfaces gérées, interdit tout trafic réseau par défaut et ne l'autorise qu'exceptionnellement (c.-à-d., interdire tout trafic, permettre le trafic par exception).

(6) L'organisation empêche toute diffusion d'information non autorisée hors des frontières du système ou toute communication non autorisée par les frontières du système en cas de défaillance opérationnelle des mécanismes de protection des frontières.

(7) Le système empêche les dispositifs distants, qui ont établi une connexion non distante avec le système, de communiquer à l'extérieur de cette voie de communication avec les ressources des réseaux externes.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle est appliquée dans le dispositif distant (p. ex., ordinateur portable) par des paramètres de configuration non modifiables par l'utilisateur. Un réseau privé virtuel est un exemple de voie de communication non distante établie à partir d'un dispositif distant. Dans ce cas, lorsque la connexion non distante est établie, les paramètres de configuration empêchent la *tunnellisation à double circuit*. Cette technique peut toutefois être utilisée par des utilisateurs distants pour communiquer avec le système d'information, comme s'il s'agissait d'une extension de celui-ci, et pour communiquer avec les ressources locales tel un serveur d'impression ou de fichiers. Puisque le dispositif distant auquel on se connecte par une connexion non distante devient une extension du système, autoriser une voie de communications double telle la tunnellisation à double circuit équivaut effectivement à permettre l'établissement de connexions externes non autorisées avec le système.

(8) Le système achemine [*Affectation : trafic de communications externe défini par l'organisation*] vers [*Affectation : réseaux externes définis par l'organisation*] par des serveurs mandataires authentifiés dans les interfaces gérées des dispositifs de protection des frontières.

Conseils supplémentaires d'amélioration : Les réseaux externes sont des réseaux qui échappent au contrôle de l'organisation. Les serveurs mandataires permettent la création de sessions TCP individuelles et le blocage d'URL, d'adresses IP et de noms de domaine particuliers. Ils sont également configurables à partir de listes de sites Web autorisés et non autorisés définies par l'organisation.

(9) Le système, au niveau des interfaces gérées, interdit le trafic réseau et identifie les utilisateurs internes (ou le code malveillant) qui représentent une menace pour les systèmes externes.

Conseils supplémentaires d'amélioration : La détection d'activités internes susceptibles de poser une menace à la sécurité des systèmes d'information externes est parfois désignée sous le nom de détection d'extrusion. Ce type de détection à la frontière du système inclut l'analyse du trafic réseau (entrant et sortant) à la recherche d'indices d'une menace interne à la sécurité des systèmes externes.

(10) L'organisation empêche l'exfiltration d'information non autorisée entre les interfaces gérées.

Conseils supplémentaires d'amélioration : Les mesures pour empêcher l'exfiltration d'information non autorisée du système d'information incluent, par exemple, (i) le respect strict des formats de protocole, (ii) la surveillance d'indices de balisage du système, (iii) la surveillance de l'utilisation de la stéganographie, (iv) la déconnexion des interfaces de réseau externe, sauf lorsqu'elles sont explicitement requises, (v) le désassemblage et l'assemblage d'en-têtes de paquet et (vi) le recours à l'analyse de profil du trafic pour détecter tout écart par rapport au volume ou aux types de trafic prévus dans l'organisation. Les exemples de dispositifs qui permettent d'imposer ce respect strict incluent les pare-feu d'inspection approfondie de paquet et les passerelles XML. Ces dispositifs vérifient le respect de la spécification du protocole au

niveau de la couche application et permettent d'identifier les vulnérabilités indétectables par des dispositifs fonctionnant au niveau de la couche réseau ou transport.

(11) Le système vérifie les communications entrantes pour s'assurer qu'elles proviennent d'une source autorisée et qu'elles sont acheminées vers une destination autorisée.

(12) Le système applique des mécanismes de protection des frontières intégrés à l'hôte pour les serveurs, les postes de travail et les dispositifs mobiles.

Conseils supplémentaires d'amélioration : Un pare-feu intégré au système hôte peut remplir le rôle joué par les mécanismes de protection des frontières utilisés dans les dispositifs mobiles, tels les portables, et les autres types de dispositifs mobiles qui utilisent ces mécanismes.

(13) L'organisation isole les [*Affectation : outils, mécanismes et composantes de soutien clés de sécurité de l'information définis par l'organisation*] des autres composantes internes de système par des sous-réseaux physiques distincts dotés d'interfaces gérées avec les autres parties du système.

(14) L'organisation assure la protection contre les connexions physiques qui traversent les mécanismes de protection des frontières intégrées aux [*Affectation : liste des interfaces gérées définie par l'organisation*].

Conseils supplémentaires d'amélioration : Les systèmes d'information fonctionnant à différents niveaux de sécurité peuvent normalement partager des contrôles physiques et environnementaux communs puisqu'ils peuvent occuper les mêmes installations et partager les mêmes salles d'équipement, cabinets de câblage et voies de distribution des câbles. Le protection contre les connexions physiques non autorisées peut être assurée, par exemple, par l'utilisation de chemins de câbles et de bâtis et de boîtiers de connexions physiquement distincts et clairement identifiés à chaque extrémité des interfaces gérées et dotés de contrôles d'accès physique qui en limitent l'accès. Contrôle connexe : PE-4.

(15) Le système achemine tous les accès privilégiés de réseau par une interface gérée spécialisée aux fins de contrôle des accès et de vérification.

Conseils supplémentaires d'amélioration : Contrôles connexes : AC-2, AC-3, AC-4, AU-2.

(16) Le système empêche le repérage de composantes de système particulières (ou dispositifs) d'une interface gérée.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle vise à protéger contre le repérage les adresses réseau des composantes de l'interface gérée à l'aide de techniques et d'outils communs servant à identifier les dispositifs d'un réseau. Les adresses réseau ne peuvent être repérées (elles ne sont ni publiées ni entrées dans le système de noms de domaine) et on doit les connaître au préalable pour accéder au réseau. Une autre technique pour camoufler ces adresses consiste à les changer périodiquement.

(17) L'organisation utilise des mécanismes automatisés pour imposer le respect strict des formats de protocole.

Conseils supplémentaires d'amélioration : Les mécanismes automatisés utilisés pour imposer le respect strict des formats de protocole incluent, par exemple, les pare-feu d'inspection approfondie des paquets et les passerelles XML. Ces dispositifs vérifient le respect de la spécification du protocole (p. ex., IEEE) au niveau de la couche application et permettent d'identifier d'importantes vulnérabilités indétectables par les dispositifs fonctionnant au niveau de la couche réseau ou transport.

(18) Le système cesse de fonctionner de façon sécuritaire dans l'éventualité d'une défaillance opérationnelle d'un dispositif de protection des frontières.

Conseils supplémentaires d'amélioration : L'arrêt sécuritaire de fonctionnement est rendue possible par l'application d'un ensemble de mécanismes qui, dans l'éventualité d'une défaillance opérationnelle d'un dispositif de protection des frontières d'une interface gérée (p. ex., routeur, pare-feu, agent de sécurité, passerelle d'application située dans un sous-réseau protégé appelé couramment zone démilitarisée), font en sorte que le système ne peut se trouver dans un état non protégé et perdre ses propriétés innées de protection de la sécurité. Toute défaillance de dispositif de protection des frontières ne doit permettre que de l'information à l'extérieur du dispositif ne puisse y pénétrer, ni permettre la diffusion non autorisée d'information.

Références :

Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22) du CSTC [Référence 42].
Isolation d'un serveur d'entreprise Blackberry dans un environnement Microsoft Exchange (ITSG-23) du CSTC [Référence 43].
Établissement des zones de sécurité dans un réseau – Considérations en matière de positionnement des services au sein de zones spécifiques (ITSG-38) du CSTC [Référence 44].

SC-8 INTÉGRITÉ DES TRANSMISSIONS

Contrôle :

(A) Le système d'information protège l'intégrité de l'information transmise.

Conseils supplémentaires : Ce contrôle s'applique aux communications dans les réseaux internes et externes. Si l'organisation recoure à un fournisseur de services commercial pour ses transmissions plutôt que de compter sur son propre service spécialisé, il peut être plus difficile d'obtenir l'assurance que les contrôles requis d'intégrité des transmissions sont effectivement appliqués. Lorsqu'il est impossible ou difficilement réalisable de se procurer ces contrôles essentiels par la voie contractuelle, l'organisation doit soit appliquer des contrôles de sécurité compensatoires appropriés, soit accepter explicitement le risque supplémentaire. Contrôles connexes : AC-17, PE-4.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes cryptographiques pour déceler toute modification apportée à l'information durant sa transmission, sauf si elle est protégée par des mesures physiques de secours. La cryptographie doit être conforme aux exigences du contrôle SC-13.

Conseils supplémentaires d'amélioration : Les mesures physiques de secours incluent, par exemple, les systèmes de diffusion protégés. Contrôle connexe : SC-13.

(2) Le système maintient l'intégrité de l'information durant les opérations de regroupement, d'emballage et de transformation préparatoires à sa transmission.

Conseils supplémentaires d'amélioration : L'information peut être modifiée intentionnellement et (ou) de façon malveillante aux points de regroupement des données ou de transformation du protocole et, ainsi, voir son intégrité compromise.

Références :

Aucune.

SC-9 CONFIDENTIALITÉ DES TRANSMISSIONS

Contrôle :

(A) Le système d'information protège la confidentialité de l'information transmise.

Conseils supplémentaires : Ce contrôle s'applique aux communications dans les réseaux internes et externes. Si l'organisation recoure à un fournisseur de services commercial pour ses transmissions plutôt que d'utiliser son propre service spécialisé, il peut être plus difficile d'obtenir l'assurance que les contrôles requis d'intégrité des transmissions sont effectivement appliqués. Lorsqu'il est impossible ou difficilement réalisable de se procurer ces contrôles essentiels par la voie contractuelle, l'organisation doit soit appliquer des contrôles de sécurité compensatoires appropriés, soit accepter explicitement le risque supplémentaire. Contrôles connexes : AC-17, PE-4.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes cryptographiques pour déceler toute modification apportée à l'information durant sa transmission, sauf si elle est protégée par [*Affectation : mesures physiques de secours définies par l'organisation*]. La cryptographie doit être conforme aux exigences du contrôle SC-13.

Conseils supplémentaires d'amélioration : Les mesures physiques de secours incluent, par exemple, les systèmes de diffusion protégés. Contrôle connexe : SC-13.

(2) Le système maintient l'intégrité de l'information durant les opérations de regroupement, d'emballage et de transformation préparatoires à sa transmission.

Conseils supplémentaires d'amélioration : L'information peut être modifiée intentionnellement et (ou) de façon malveillante aux points de regroupement des données ou de transformation du protocole et, ainsi, voir son intégrité compromise.

(100) L'organisation recoure à des mécanismes de sécurité du flux de trafic pour protéger les communications contre des attaques par analyse de flux.

Conseils supplémentaires d'amélioration : La sécurité du flux de trafic protège les organisations contre la surveillance passive des caractéristiques des communications et peut être appliquée au trafic des utilisateurs et à l'information de contrôle de l'infrastructure du réseau . De manière générale, cette amélioration s'applique seulement aux systèmes d'information classifiée et doit être appliquée en recourant à une solution approuvée par le CSTC.

Références :

Norme opérationnelle de sécurité – Gestion de la sécurité des technologies de l'information du SCT [Référence 8].
Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés (ITSA-11D) du CSTC [Référence 9].
Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B (ITSB-40) du CSTC [Référence 29].

SC-10 DÉCONNEXION DE RÉSEAU

Contrôle :

(A) Le système d'information met un terme à toute connexion réseau associée à une session de communications à la fin de la session ou après [*Affectation : durée définie par l'organisation*] d'inactivité.

Conseils supplémentaires : Ce contrôle s'applique aux réseaux internes et externes. L'interruption des connexions réseau associées à une session de communications incluent, par exemple, la libération des paires d'adresses TCP et ports IP au niveau du système d'exploitation, ou la libération des attributions réseau au niveau de l'application lorsque de multiple sessions d'application utilisent une seule connexion réseau du système d'exploitation. La durée de la période d'inactivité peut, selon que l'organisation le juge nécessaire, être fixée en fonction des durées associées au type d'accès réseau ou à des accès spécifiques.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-11 CHEMIN DE CONFIANCE

Contrôle :

(A) Le système d'information établit une voie de communication fiable entre l'utilisateur et les fonctions de sécurité de système suivantes : [*Affectation : fonctions de sécurité définies par l'organisation et incluant, au minimum, l'authentification et la réauthentification du système*].

Conseils supplémentaires : Un chemin de confiance est utilisé pour établir des connexions de niveau de fiabilité élevé entre les fonctions de sécurité du système et l'utilisateur (p. ex., ouvertures de session).

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-12 ÉTABLISSEMENT ET GESTION DES CLÉS DE CHIFFREMENT

Contrôle :

(A) L'organisation établit et gère les clés de chiffrement utilisées pour les opérations de cryptographie requises dans le système d'information.

Conseils supplémentaires : L'établissement et la gestion des clés de chiffrement peuvent être effectués en utilisant des procédures manuelles ou des mécanismes automatisés soutenus par des procédures manuelles. En plus d'être essentielle au bon fonctionnement des mécanismes cryptographiques, la gestion efficace des clés de chiffrement permet de garantir le maintien de la disponibilité de l'information dans l'éventualité où les utilisateurs perdent leurs clés. La cryptographie doit être conforme aux exigences du contrôle SC-13. Contrôle connexe : SC-13.

Améliorations du contrôle :

(1) L'organisation maintient la disponibilité de l'information dans l'éventualité où les utilisateurs perdent leurs clés de chiffrement.

(2) L'organisation produit, contrôle et distribue les clés de chiffrement symétriques en utilisant une technologie et des processus de gestion des clés approuvés par le CSTC.

Conseils supplémentaires d'amélioration : Contrôle connexe : SC-13.

(3) L'organisation produit, contrôle et distribue les clés de chiffrement symétriques et asymétriques en utilisant une technologie et des processus de gestion des clés approuvés par le CSTC.

Conseils supplémentaires d'amélioration : Contrôle connexe : SC-13.

(4) L'organisation produit, contrôle et distribue les clés de chiffrement asymétriques en utilisant des certificats approuvés d'assurance de niveau moyen ou du matériel de chiffrement prépositionné.

(5) L'organisation produit, contrôle et distribue les clés de chiffrement asymétriques en utilisant des certificats approuvés d'assurance de niveau moyen ou élevé et des jetons de sécurité matériels qui protègent la clé privée de l'utilisateur.

Références :

Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés (ITSA-11D) du CSTC [Référence 9].
Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B (ITSB-40) du CSTC [Référence 29].
Manuel de contrôle du matériel COMSEC (ITSG-10) du CSTC [Référence 37].
Manuel sur la commande de clés cryptographiques (ITSG-13) du CSTC [Référence 40].

SC-13 UTILISATION DE LA CRYPTOGRAPHIE

Contrôle :

(A) Le système d'information applique des protections cryptographiques fondées sur des systèmes de chiffrement conformes aux lois du GC et aux politiques, directives et normes concernées du SCT.

Conseils supplémentaires : Le contrôle de base, sans amélioration, ne requiert pas de cryptographie validée par le PVMC. Toutefois, il exige l'utilisation d'algorithmes cryptographiques approuvés par le CSTC qui incluent, en plus des algorithmes, des longueurs de clé, des cryptopériodes, des modes d'opération, des schémas de

remplissage et un générateur de nombres aléatoires approuvé, tel que décrit dans le document *Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés (ITSA-11D) du CSTC* [Référence 9]. On recommande également de choisir les améliorations appropriées pour protéger les données sensibles.

Améliorations du contrôle :

(1) L'organisation utilise, au minimum, la cryptographie validée par le PVMC pour protéger les données non classifiées mais sensibles (à l'exclusion des données classifiées et protégées).

Conseils supplémentaires d'amélioration : Le Programme de validation des modules cryptographiques (PVMC) est un produit développé conjointement par le Centre de la sécurité des télécommunications Canada (CSTC) et le National Institute of Standards and Technology (NIST). Il valide les modules cryptographiques en vérifiant leur conformité à la norme 140-2, Security Requirements for Cryptographic Modules, des FIPS (Federal Information Processing Standards), et autres normes FIPS sur la cryptographie. On attribue aux modules cryptographiques validés en vertu du PVMC un numéro de certificat unique, publié sur le site Web du NIST.

(2) L'organisation utilise une cryptographie approuvée par le CSTC pour protéger les données classifiées.

Conseils supplémentaires d'amélioration : La cryptographie approuvée par le CSTC exige une certification par une autorité COMSEC nationale approuvée pour l'équipement cryptographique de Type 1 (ou équivalent) et un certificat d'approbation d'utilisation (AFU) du CSTC pour l'approbation de la configuration de l'équipement et le plan de gestion des clés. Communiquer avec le CSTC pour plus de détails.

(3) L'organisation utilise, au minimum, une cryptographie validée par le PVMC pour protéger les données qui doivent être mises hors de la portée des individus qui possèdent la cote de sécurité appropriée mais non les autorisations d'accès requises.

(4) L'organisation utilise une cryptographie [*Sélection : validée par le PVMC; approuvée par le CSTC*] pour l'application des signatures numériques.

(100) L'organisation utilise une cryptographie validée par le PVMC pour protéger les données protégées A en transit.

(101) L'organisation utilise cryptographie validée par le PVMC pour protéger les données protégées B en transit.

(102) L'organisation utilise une cryptographie approuvée par le CSTC pour protéger les données protégées C en transit.

(103) L'organisation utilise une cryptographie [*Sélection : validée par le PVMC; approuvée par le CSTC*] pour protéger les données [*Sélection : données définies par l'organisation*] inactives.

(104) L'organisation utilise l'équipement COMSEC en conformité avec les *Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada (ITSD-01) du CSTC* [Référence 15].

Références :

Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés (ITSA-11D) du CSTC [Référence 9].
Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B (ITSB-40) du CSTC [Référence 29].
*Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada (ITSD-01) du CSTC [*Référence 15].
Guide to Interconnecting Security Domains (ITSG-32) du CSTC [Référence 23].

SC-14 PROTECTION DE L'ACCÈS PUBLIC

Contrôle :

(A) Le système d'information protège l'intégrité et la disponibilité de l'information et des applications accessibles au public.

Conseils supplémentaires : Le but de ce contrôle est de s'assurer que les organisations s'intéressent explicitement aux besoins de protection de l'information et des applications accessibles au public et intègrent éventuellement ces mécanismes aux autres contrôles de sécurité.

Améliorations du contrôle :

Aucune.

Références :

Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22) du CSTC [Référence 42].
Établissement des zones de sécurité dans un réseau – Considérations en matière de positionnement des services au sein de zones spécifiques (ITSG-38) du CSTC [Référence 44].

SC-15 DISPOSITIFS D'INFORMATIQUE COOPÉRATIVE

Contrôle :

(A) Le système d'information interdit l'activation à distance des dispositifs d'informatique coopérative, sauf dans les situations suivantes : [*Affectation : exceptions définies par l'organisation pour lesquelles l'activation à distance doit être permise*].

(B) Le système d'information indique de manière explicite l'utilisation permise de ces dispositifs par ceux qui se trouvent à proximité physique de la ressource.

Conseils supplémentaires : Les dispositifs d'informatique coopérative incluent, par exemple, les tableaux blancs virtuels, les caméras et les microphones en réseau. L'indication de l'utilisation de manière explicite inclut, par exemple, des avertissements aux utilisateurs lorsque les dispositifs sont activés.

Améliorations du contrôle :

(1) Le système facilite aux utilisateurs la déconnexion physique des dispositifs d'informatique coopérative.

(2) Le système ou l'environnement de soutien bloquent le trafic entrant et sortant entre les clients de messagerie instantanée configurés indépendamment par les utilisateurs ultimes et les fournisseurs de services externes.

Conseils supplémentaires d'amélioration : Les restrictions concernant le blocage n'incluent pas les services de messagerie instantanée configurés par une organisation pour exécuter une fonction autorisée.

(3) L'organisation désactive ou retire les dispositifs d'informatique coopérative des systèmes d'information dans les réseaux dont le niveau de classification est inférieur à [*Affectation : niveau de classification*] et qui se trouvent dans [*Affectation : zones de travail protégées définies par l'organisation*].

Références :

Aucune.

SC-16 TRANSMISSION DES ATTRIBUTS DE SÉCURITÉ

Contrôle :

(A) Le système d'information associe des attributs de sécurité à l'information échangée entre les systèmes d'information.

Conseils supplémentaires : Les attributs de sécurité peuvent être explicitement ou implicitement associés à l'information contenue dans le système d'information. Contrôle connexe : AC-16.

Améliorations du contrôle :

(1) Le système valide l'intégrité des attributs de sécurité échangés entre les systèmes.

Références :

Aucune.

SC-17 CERTIFICATS D'INFRASTRUCTURE À CLÉ PUBLIQUE

Contrôle :

(A) L'organisation émet des certificats à clé publique en vertu de la [*Affectation : politique de certification définie par l'organisation*] ou les obtient en vertu d'une politique de certification appropriée d'un fournisseur de services autorisé.

Conseils supplémentaires : Pour ce qui est des certificats d'utilisateur, chaque organisation soit établit une autorité de certification organisationnelle cocertifiée avec l'Autorité de cocertification fédérale canadienne, soit utilise les certificats d'un fournisseur de services autorisé.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-18 CODE MOBILE

Contrôle :

(A) L'organisation définit le code mobile et les technologies de code mobile acceptables et inacceptables.

(B) L'organisation définit les restrictions d'utilisation et donne des conseils sur l'utilisation du code mobile et des technologies de code mobile acceptables.

(C) L'organisation autorise, surveille et contrôle l'utilisation du code mobile dans le système d'information.

Conseils supplémentaires : Les décisions concernant le recours à du code mobile dans les systèmes organisationnels doivent tenir compte de la possibilité qu'une utilisation malveillantes du code cause des dommages au système. Les technologies de code mobile incluent, par exemple, Java, JavaScript, ActiveX, PDF, Postscript, films Shockwave, animations Flash et VBScript. Les restrictions d'utilisation et les conseils sur l'utilisation du code mobile s'appliquent à la fois à la sélection et à l'utilisation du code mobile installé dans les serveurs de l'organisation et du code mobile téléchargé et exécuté dans les postes de travail individuels. La politique et les procédures concernant le code mobile visent à prévenir le développement, l'acquisition ou l'insertion de code mobile inacceptable dans le système.

Améliorations du contrôle :

(1) Le système applique des mécanismes de détection et d'inspection pour identifier le code mobile non autorisé et prendre des mesures correctrices, le cas échéant.

Conseils supplémentaires d'amélioration : Les mesures correctrices à prendre lorsque du code mobile non autorisé est détecté incluent, par exemple, le blocage, la mise en quarantaine ou l'avertissement de l'administrateur. Les transferts interdits incluent, par exemple, l'envoi de fichiers de traitement de texte qui incluent des macros.

(2) L'organisation veille à ce que l'acquisition, le développement et (ou) l'utilisation de code mobile qui sera déployé dans les systèmes répondent aux [*Affectation : exigences définies par l'organisation concernant le code mobile*].

(3) Le système empêche le téléchargement et l'exécution de tout code mobile interdit.

(4) Le système empêche l'exécution automatique de code mobile dans [*Affectation : applications logicielles définies par l'organisation*] et exige que [*Affectation : mesures définies par l'organisation*] soient prises avant d'exécuter le code.

Conseils supplémentaires d'amélioration : Les mesures requises avant l'exécution du code mobile incluent, par exemple, l'affichage d'un message de guidage aux utilisateurs avant l'ouverture des pièces jointes d'un courriel.

Références :

Aucune.

SC-19 VOIX SUR IP

Contrôle :

(A) L'organisation définit les restrictions d'utilisation et donne des conseils sur l'utilisation des technologies de voix sur IP en tenant compte de la possibilité qu'une utilisation malveillante de ces technologies cause des dommages au système d'information.

(B) L'organisation autorise, surveille et contrôle l'utilisation de la voix sur IP dans le système d'information.

Conseils supplémentaires : Aucune.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-20 SERVICE SÉCURISÉ DE RÉSOLUTION DE NOM ET (OU) D'ADRESSE (SOURCE AUTORISÉE)

Contrôle :

(A) Le système d'information produit des éléments additionnels d'information sur l'origine et l'intégrité des données en plus des données faisant autorité qu'il retourne en réponse aux demandes de résolution de nom et d'adresse.

Conseils supplémentaires : Ce contrôle permet à des clients distants d'obtenir des assurances concernant l'authentification de l'origine et la vérification de l'intégrité de l'information de résolution de nom d'hôte et (ou) de service et d'adresse réseau produite par le service. Le serveur DNS est un exemple de système d'information qui offre un service de résolution de nom et d'adresse. Les signatures numériques et les clés de chiffrement sont des exemples d'éléments additionnels d'information. Les dossiers de ressources DNS sont des exemples de données faisant autorité. Les systèmes d'information qui utilisent des technologies autres que le DNS pour mapper les noms d'hôte et (ou) de service et les adresses réseau offrent d'autres moyens de s'assurer de l'authenticité et de l'intégrité des réponses.

Améliorations du contrôle :

(1) Le système, lorsqu'il est utilisé dans un espace de nom hiérarchique distribué, offre des moyens d'indiquer l'état de sécurité des sous-espaces enfants et (si l'enfant offre des services sécurisés de résolution) de vérifier l'existence d'une chaîne de confiance entre les domaines parents et enfants.

Conseils supplémentaires d'amélioration : Un exemple de moyen d'indiquer l'état de sécurité des sous-espaces enfants est l'utilisation des dossiers de ressources de signataire de délégation du service DNS.

(100) Il est interdit d'utiliser un service VoIP non classifié dans des installations classifiées sauf si ce service est converti en service téléphonique de base (POTS) avant de quitter la frontière de l'installation.

(101) Le service VoIP est interdit dans un réseau local doté d'un accès à un réseau public de données.

Références :

Aucune.

SC-21 SERVICE SÉCURISÉ DE RÉSOLUTION DE NOM ET (OU) D'ADRESSE (RÉSOLVEUR RÉCURSIF OU CACHE)

Contrôle :

(A) Le système d'information authentifie l'origine et vérifie l'intégrité des données des réponses de résolution de nom et d'adresse qu'il reçoit de sources autorisées suite à des demandes des systèmes clients.

Conseils supplémentaires : Le serveur DNS résolveur récursif ou cache est un exemple de système d'information qui offre un service de résolution de nom et d'adresse aux clients locaux. Les serveurs DNS autorisés sont des exemples de sources faisant autorité. Les systèmes d'information qui utilisent des technologies autres que le DNS pour mapper les noms d'hôte et (ou) de service et les adresses réseau offrent d'autres moyens de s'assurer de l'authenticité et de l'intégrité des réponses.

Améliorations du contrôle :

(1) Le système authentifie l'origine et vérifie l'intégrité des données de toutes les réponses de résolution, que les demandes de service proviennent explicitement ou non de clients locaux.

Conseils supplémentaires d'amélioration : Les clients locaux incluent, par exemple, les résolveurs DNS basiques.

Références :

Aucune.

SC-22 ARCHITECTURE ET FOURNITURE DE SERVICE DE RÉSOLUTION DE NOM ET (OU) D'ADRESSE

Contrôle :

(A) Les systèmes d'information qui offrent collectivement des services de résolution de nom et d'adresse pour une organisation sont tolérants aux pannes et appliquent une séparation des rôles internes et externes.

Conseils supplémentaires : Le serveur DNS est un exemple de système d'information qui offre un service de résolution de nom et d'adresse. Il élimine les points de défaillance uniques et améliore la redondance en recourant (normalement) à au moins deux serveurs DNS autorisés dont l'un est configuré comme serveur principal et l'autre, comme serveur secondaire. En outre, les deux serveurs sont habituellement hébergés dans deux sous-réseaux différents séparés géographiquement (c.-à-d., non situés dans la même installation physique). Pour ce qui est de la séparation des rôles, les serveurs DNS associés à un rôle interne exécutent uniquement le processus de résolution de nom et d'adresse pour les demandes provenant de l'intérieur de l'organisation (c.-à-d., les clients internes). Les serveurs DNS associés à un rôle externe traitent uniquement les demandes de résolution des clients à l'extérieur de l'organisation (c.-à-d., en provenance de réseaux externes, incluant Internet). L'ensemble des clients qui peuvent accéder à un serveur DNS autorisé associé à un rôle particulier est déterminé par l'organisation (p. ex., selon une gamme d'adresses, des listes explicites).

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-23 AUTHENTICITÉ DES SESSIONS

Contrôle :

(A) Le système d'information prévoit des mécanismes pour protéger l'authenticité des sessions de communications.

Conseils supplémentaires : Ce contrôle met l'accent sur la protection des communications au niveau de la session plutôt qu'à celui des paquets. Son but est de démontrer la présence d'un lien de confiance en l'identité permanente de l'autre partie à chaque extrémité d'une session de communications et en la validité de l'information transmise. Par exemple, le contrôle intervient dans les cas d'attaques par interception, incluant le piratage de session ou l'insertion de faux renseignements dans une session. L'organisation recoure à ce contrôle seulement là où elle le juge nécessaire (p. ex., sessions d'architectures qui fournissent des services Web).

Améliorations du contrôle :

(1) Le système invalide les identificateurs de session lorsque l'utilisateur se déconnecte ou à la fin des sessions.

(2) Le système offre automatiquement une capacité de déconnexion lorsque l'utilisateur recoure à l'authentification pour accéder à des pages Web.

(3) Le système produit un identificateur de session unique pour chaque session et reconnaît uniquement les identificateurs qu'il produit.

(4) Le système produit des identificateurs de session uniques en se fondant sur [*Affectation : exigences définies par l'organisation concernant le caractère aléatoire des identificateurs*].

Conseils supplémentaires d'amélioration : L'utilisation du concept aléatoire pour la production d'identificateurs de session uniques permet de protéger le système contre les attaques de force brute visant à déterminer les futurs identificateurs de session.

Références :

Aucune.

SC-24 DÉFAILLANCE DANS UN ÉTAT CONNU

Contrôle :

(A) Le système d'information tombe en [*Affectation : état connu défini par l'organisation]* pour *[Affectation : types de défaillance définis par l'organisation*] et conserve [*Affectation : information sur l'état du système définie par l'organisation*] durant la défaillance.

Conseils supplémentaires : La défaillance du système dans un état connu peut protéger sa sûreté ou sa sécurité en conformité avec la mission et (ou) les besoins opérationnels de l'organisation. Ainsi, on prévient la perte de confidentialité, d'intégrité ou de disponibilité dans l'éventualité d'une défaillance du système ou d'une de ses composantes. Ce type de défaillance permet d'empêcher les systèmes de tomber en panne dans un état susceptible de causer des préjudices aux individus ou à la propriété. La protection de l'état du système facilite le redémarrage et le retour au mode opérationnel de l'organisation tout en perturbant le moins possible les processus liés à la mission et aux opérations.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-25 NŒUDS LÉGERS

Contrôle :

(A) Le système d'information utilise des composantes de traitement qui utilisent un minimum de fonctions et de capacité de stockage.

Conseils supplémentaires : Le déploiement de composantes de système qui utilisent un minimum de fonctions (p. ex., nœuds sans disque et technologies de client léger) atténue l'importance de protéger le point d'extrémité de chaque utilisateur ainsi que les possibilités d'exposition de l'information, des systèmes et des services à toute attaque qui aurait réussi. Contrôle connexe : SC-30.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-26 PIÈGES À PIRATES

Contrôle :

(A) Le système d'information inclut des composantes conçues spécifiquement pour servir de cibles aux attaques malveillantes afin d'être en mesure de les détecter, les repousser et les analyser.

Conseils supplémentaires : Aucune.

Améliorations du contrôle :

(1) Le système inclut des composantes qui tentent proactivement d'identifier tout code malveillant en provenance du Web

Conseils supplémentaires d'amélioration : Les dispositifs qui tentent activement d'identifier le code malveillant en provenance du Web en se faisant passer pour des clients sont appelés pièges clients ou pièges.

Références :

Aucune.

SC-27 APPLICATIONS INDÉPENDANTES DES SYSTÈMES D'EXPLOITATION

Contrôle :

(A) Le système d'information inclut : [*Affectation : applications définies par l'organisation qui sont indépendantes des systèmes d'exploitation*].

Conseils supplémentaires : Les applications indépendantes des systèmes d'exploitation sont des applications qui peuvent fonctionner sous plusieurs systèmes d'exploitation. Elles favorisent la portabilité et la reconstitution sur

des architectures de plates-formes différentes, augmentant ainsi la disponibilité des fonctions essentielles d'une organisation lorsque des attaques sont lancées contre ses systèmes qui fonctionnent sous un système d'exploitation particulier.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-28 PROTECTION DE L'INFORMATION INACTIVE

Contrôle :

(A) Le système d'information protège la confidentialité et l'intégrité de l'information inactive.

Conseils supplémentaires : Le but de ce contrôle est d'assurer la confidentialité et l'intégrité de l'information inactive (d'utilisateur et de système) contenue dans des dispositifs fixes. L'information inactive désigne l'état des renseignements contenus dans les dispositifs de stockage secondaires (p. ex., lecteur de disque, de bande, etc.) d'un système d'information organisationnel. Les configurations et (ou) les ensembles de règles (développées pour les pare-feu, les passerelles, les systèmes de détection et (ou) de prévention des intrusions) et les routeurs à filtrage et les contenus d'authentifiant sont des exemples d'information système susceptible de nécessiter une protection. Les organisations peuvent choisir, à leur discrétion, d'utiliser différents mécanismes de protection de la confidentialité et de l'intégrité. Contrôle connexe : SC-13.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes cryptographiques pour empêcher la divulgation et la modification non autorisées de l'information inactive qui n'est pas déjà protégée par des mesures physiques de secours. La cryptographie est conforme aux exigences du contrôle SC-13.

Références :

Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements protégés (ITSA-11D) du CSTC [Référence 9].
Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B (ITSB-40) du CSTC [Référence 29].

SC-29 HÉTÉROGÉNÉITÉ

Contrôle :

(A) L'organisation utilise diverses technologies de l'information pour la mise en œuvre du système d'information.

Conseils supplémentaires : Accroître la diversité des technologies utilisées dans les systèmes d'information réduit l'incidence de l'exploitation d'une technologie particulière. Les organisations qui optent pour ce contrôle doivent tenir compte de la possibilité qu'une plus grande diversité peut accroître la complexité et les tâches de gestion, éléments susceptibles d'entraîner des erreurs et des configurations inadéquates et d'augmenter le risque global.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-30 TECHNIQUES DE VIRTUALISATION

Contrôle :

(A) L'organisation utilise des techniques de virtualisation pour maquiller les composantes du système et laisser croire qu'il s'agit d'autres types de composantes ou de composantes possédant des configurations différentes.

Conseils supplémentaires : Les techniques de virtualisation permettent aux organisations de camoufler les systèmes d'information et, éventuellement, de réduire la probabilité d'attaques réussies sans encourir les coûts associés à la mise en place de plate-formes multiples.

Améliorations du contrôle :

(1) L'organisation utilise des techniques de virtualisation pour faciliter le déploiement de divers systèmes d'exploitation et applications qui ont été modifiés [*Affectation : fréquence définie par l'organisation*].

Conseils supplémentaires d'amélioration : Les modifications fréquentes des systèmes d'exploitation et des applications posent des défis au plan de la gestion de la configuration mais ont l'avantage de compliquer la tâche des adversaires qui souhaitent réussir leurs attaques. Modifier les systèmes d'exploitation ou les applications de manière apparente plutôt que réelle exige uniquement des changements de nature virtuelle qui contribuent à la fois à rendre difficile la réussite des attaques de pirates et à réduire le travail de gestion de la configuration.

(2) L'organisation utilise une approche aléatoire pour la mise en œuvre des techniques de virtualisation.

Références :

Aucune.

SC-31 ANALYSE DES VOIES CLANDESTINES

Contrôle :

(A) L'organisation exige des développeurs et (ou) intégrateurs de système d'information qu'ils effectuent une analyse des voies clandestines afin d'identifier les aspects des communications système susceptibles de servir de voies potentielles au stockage clandestin et aux canaux temporels cachés.

Conseils supplémentaires : Les développeurs et (ou) intégrateurs de système d'information sont les mieux placés pour déterminer les voies du système susceptibles d'être converties en voies clandestines. L'analyse des voies clandestines est une activité significative en présence de flux d'information inter-domaines non autorisés, par exemple, les systèmes qui contiennent de l'information destinée à l'exportation et qui sont connectés à des réseaux externes (c.-à-d., réseaux non contrôlés par l'organisation). Elle est également significative dans le cas des systèmes à sécurité multiniveaux et des systèmes inter-domaines.

Améliorations du contrôle :

(1) L'organisation teste un sous-ensemble de voies clandestines identifiées par le fournisseur afin de déterminer si elles sont exploitables.

Références :

Aucune.

SC-32 PARTITIONNEMENT DES SYSTÈMES D'INFORMATION

Contrôle :

(A) L'organisation partitionne au besoin le système d'information en composantes hébergées dans des domaines (ou environnements) physiques distincts.

Conseils supplémentaires : Le partitionnement du système d'information fait partie de la stratégie de protection en profondeur. Une évaluation organisationnelle des risques permet de déterminer le partitionnement des composantes en domaines (ou environnements) physiques distincts. Les catégories de sécurité permettent également de décider des composantes qui se prêtent le mieux au partitionnement de domaine. Les interfaces gérées limitent ou interdisent l'accès réseau et les flux d'information entre les composantes partitionnées du système. Contrôles connexes : AC-4, SC-7.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-33 INTÉGRITÉ DE LA PRÉPARATION DES TRANSMISSIONS

Contrôle :

(A) Le système d'information protège l'intégrité de l'information durant le processus de regroupement, d'emballage et de transformation des données en vue de leur transmission.

Conseils supplémentaires : L'information peut faire l'objet de modifications non autorisées (p. ex., malveillantes et (ou) accidentelles) au stade de regroupement des données ou aux points de transformation du protocole.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SC-34 PROGRAMMES EXÉCUTABLES NON MODIFIABLES

Contrôle :

(A) Le système d'information, au niveau de [*Affectation : composantes de système définies par l'organisation*], charge et exécute l'environnement d'exploitation à partir de supports matériels non inscriptibles.

(B) Le système d'information, au niveau de [*Affectation : composantes de système définies par l'organisation*], charge et exécute [*Affectation : applications définies par l'organisation*] à partir de supports matériels non inscriptibles.

Conseils supplémentaires : Dans ce contrôle, le terme environnement d'exploitation désigne le code qui héberge les applications, par exemple, un système d'exploitation qui gère et surveille l'application ou une application fonctionnant directement dans la plate-forme matérielle. Les supports matériels non inscriptibles incluent, par

exemple, les lecteurs CD-R et DVD-R. L'utilisation de dispositifs de stockage non modifiables assure l'intégrité du programme logiciel dès le point de création de l'image non inscriptible.

Améliorations du contrôle :

(1) L'organisation utilise [*Affectation : composantes de système définies par l'organisation*] avec des dispositifs de stockage qui demeurent non inscriptibles à chaque redémarrage de la composante ou lors des mises sous tension et hors tension.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle (i) élimine la possibilité d'insertion de code malveillant par un dispositif de stockage non inscriptible persistant de la composante désignée et (ii) n'exige pas l'utilisation de ce type de dispositif (exigence applicable directement ou en vertu d'une restriction particulière imposée par le contrôle AC-19).

(2) L'organisation protège l'intégrité de l'information contenue dans les supports non inscriptibles.

Conseils supplémentaires d'amélioration : Cette amélioration de contrôle inclut la protection de l'intégrité de l'information qui sera copiée dans les supports non inscriptibles et le contrôle des supports après l'enregistrement de l'information. Les mesures de protection peuvent inclure, selon que l'organisation le juge nécessaire, une combinaison de mécanismes de prévention et de détection et (ou) d'intervention. Cette amélioration peut être satisfaite par les exigences imposées par d'autres contrôles tels les contrôles AC-3, AC-5, CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SA-12, SC-28, SI-3 et SI-7.

Références :

Aucune.

SC-100 AUTHENTIFICATION DES SOURCES

Contrôle :

(A) Le système d'information permet au destinataire d'un message de vérifier l'identificateur présumé de la source dans un message.

Conseils supplémentaires : L'authentification des sources empêche toute partie non autorisée d'envoyer un message en se faisant passer pour une autre. Ce contrôle s'applique aux communications non liées à une session et peut être appliqué aux protocoles de n'importe quelle couche, des paquets IP au courrier électronique. Contrôles connexes : IA-1, IA-2, IA-3, IA-4, IA-5, SC-8, SC-13.

Améliorations du contrôle :

(1) L'authentification de l'identificateur présumé du message fait appel à la cryptographie.

(2) L'organisation utilise la cryptographie validée par le PVMC pour la création et la vérification des signatures numériques. Voir le contrôle SC-13.

(3) L'organisation utilise la cryptographie approuvée par le CSTC et les protocoles pour effectuer l'authentification. Voir le contrôle SC-13.

Références :

Aucune.

SC-101 – SYSTÈMES DE TÉLÉCOMMUNICATIONS NON CLASSIFIÉS DANS LES INSTALLATIONS PROTÉGÉES

Contrôle :

(A) Les systèmes de télécommunications non classifiés dans les installations protégées ne doivent ni laisser passer ni transmettre de discussions audio sensibles lorsqu'ils sont désactivés et inutilisés. En plus, ils doivent être configurés de manière à empêcher toute activation ou contrôle externes. Les concepts de

protection audio de type « combiné raccroché » mentionnés dans les normes 2 et 6 du groupe de sécurité de téléphonie (TSG) doivent être intégrés aux systèmes de télécommunications des installations SCI.

(B) Les systèmes et services téléphoniques non classifiés doivent être configurés de manière à empêcher les exploits techniques ou la pénétration. En plus, ils doivent intégrer des contrôles d'accès physique et logiciels pour empêcher la divulgation ou la manipulation de la programmation système et des données stockées.

(C) L'organisation doit s'assurer d'appliquer aux systèmes de télécommunications non classifiés les exigences spécifiques suivantes :

(a) Assurer la protection audio de type « combiné raccroché » par l'utilisation d'instrument(s) TSG 6, de dispositifs de déconnexion approuvés TSG 6, ou d'une configuration de système TSG 2 équivalente.

(b) Assurer l'isolation par l'utilisation d'un système téléphonique informatisé (CTS) doté d'un contrôle de configuration logiciel et matériel et d'un contrôle des rapports de vérification (enregistrement détaillé des données d'appel, rapports sur les données d'appel, etc.). La programmation système ne doit pas permettre de placer ou de maintenir le combiné en position non raccrochée. La configuration du système doit faire en sorte d'identifier et d'atténuer toutes les vulnérabilités associées à l'état du combiné (raccroché ou non).

(c) Veiller à ce que l'équipement utilisé pour administrer les systèmes téléphoniques soit installé dans une zone dont l'accès est réservé au personnel autorisé. Lorsque les terminaux d'administration locaux (d'un CTS) ne sont pas ou ne peuvent être hébergés dans la zone contrôlée ni protégés contre les manipulations non autorisées, on doit exiger l'utilisation d'appareils téléphoniques approuvés TSG 6, quelle que soit la configuration du CTS.

(d) Veiller à ne pas recourir à la maintenance à distance hors de l'installation protégée.

(e) Veiller à ne pas utiliser de téléphones à haut-parleur ni de systèmes d'audioconférences avec les systèmes de télécommunications non classifiés dans les installations SCI. Les exceptions à cette exigence peuvent être approuvées par le CSTC dans le cas où il y a une isolation audio suffisante entre ces systèmes et les autres pièces de discussion classifiée dans l'installation SCI et lorsque l'on a établi des procédures pour empêcher la transmission par inadvertance d'information classifiée.

(f) Veiller à ce que les fonctions utilisées pour la messagerie vocale ou les systèmes unifiés de messagerie soient configurées de manière à empêcher l'accès non autorisé aux ports de diagnostic distants ou à la tonalité de manœuvre interne.

(g) Veiller à ce que les répondeurs téléphoniques (TAD) et les télécopieurs ne soient pas dotés de fonctions qui présentent des vulnérabilités au plan de la sécurité, p. ex., surveillance des locaux à distance, programmation à distance, ou autres fonctions similaires qui peuvent permettre un accès à distance aux caractéristiques audio de la pièce. Le CSTC doit donner son approbation avant l'installation ou l'utilisation de tels dispositifs.

(D) Tous les systèmes de télécommunications non classifiés et leurs infrastructures doivent être isolés physiquement et électriquement de tout système d'information classifiée et (ou) de télécommunications, conformément aux exigences du National Security Telecommunications and Information Systems Security Committee ou de toute autre norme d'isolation appliquée au système d'information classifiée en place.

Conseils supplémentaires : Aucune.

Améliorations du contrôle :

Aucune.

Références :

DCID 6/9 Physical Security Standards for Sensitive Compartmented Information Facilities [Référence 56].
NTSWG TSG Standard 2 Guidelines for Computerized Telephone Systems [Référence 57].
NTSWG TSG Standard 6 TSG-Approved Equipment [Référence 58].

4.17 FAMILLE : INTÉGRITÉ DE L'INFORMATION ET DES SYSTÈMES

CLASSE : OPÉRATIONNELLE

SI-1 POLITIQUE ET PROCÉDURES D'INTÉGRITÉ DE L'INFORMATION ET DES SYSTÈMES

Contrôle :

(A) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] une politique d'intégrité de l'information et des systèmes formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité).

(B) L'organisation développe, diffuse et examine et (ou) met à jour [*Affectation : fréquence définie par l'organisation*] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique d'intégrité de l'information et des systèmes et des contrôles correspondants.

Conseils supplémentaires : Le but de ce contrôle est de créer la politique et les procédures nécessaires à la mise en œuvre efficace de divers contrôles, incluant les améliorations, de la famille des contrôles de l'intégrité de l'information et des systèmes. La politique et les procédures de contrôle d'accès sont conformes aux lois du GC et aux politiques, directives et normes concernées du SCT. Les politiques et procédures organisationnelles existantes peuvent rendre inutiles toute politique et procédure supplémentaires spécifiques. La politique d'intégrité de l'information et des systèmes peut être incluse dans la politique générale de sécurité de l'information de l'organisation. Les procédures d'intégrité de l'information et des systèmes peuvent être développées pour le programme de sécurité général et pour un système d'information particulier, le cas échéant. La stratégie organisationnelle de gestion du risque est un facteur clé du développement de la politique d'intégrité de l'information et des systèmes. Contrôle connexe : PM-9.

Améliorations du contrôle :

Aucune.

Références :

*Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [*Référence 8].

SI-2 CORRECTION DES LACUNES

Contrôle :

(A) L'organisation identifie, signale et corrige les lacunes du système d'information.

(B) L'organisation, avant leur installation, teste les rustines logicielles de correction des lacunes pour en vérifier l'efficacité et les répercussions potentielles sur ses systèmes d'information.

(C) L'organisation intègre le mécanisme de correction des lacunes à son processus de gestion de la configuration.

Conseils supplémentaires : L'organisation identifie les systèmes d'information dont le logiciel est visé par les lacunes récemment annoncées (et par les vulnérabilités potentielles qui leur sont associées) et transmet cette information aux agents désignés responsables de la sécurité de l'information (p. ex., agents principaux de sécurité de l'information, gestionnaires de la sécurité des systèmes d'information, agents de la sécurité des systèmes

d'information). L'organisation (incluant tout entrepreneur à son service) installe dans les plus brefs délais les mises à jour logicielles de sécurité (p. ex., rustines, service packs et réparations à chaud). Elle corrige également le plus rapidement possible les lacunes relevées durant les évaluations de sécurité, la surveillance permanente, les activités liées aux interventions en cas d'incident ou le processus de traitement des erreurs. À cet égard, on incite les organisations à utiliser des bases de données telles celles des listes CWE ou CVE. En imposant l'intégration des mécanismes de correction des lacunes au processus de gestion de la configuration de l'organisation, le contrôle vise à s'assurer du suivi et de la vérification des mesures correctrices requises ou anticipées. Contrôles connexes : CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.

Améliorations du contrôle :

(1) L'organisation centralise la gestion du processus de correction des lacunes et installe les mises à jour logicielles automatiquement.

Conseils supplémentaires d'amélioration : Compte tenu de l'importance de maintenir l'intégrité et la disponibilité du système, les organisations doivent prendre soin de bien choisir la méthodologie de mise à jour automatique.

(2) L'organisation utilise des mécanismes automatisés [*Affectation : fréquence définie par l'organisation*] pour déterminer l'état des composantes de système avant de procéder à la correction des lacunes.

(3) L'organisation mesure le temps écoulé entre l'identification des lacunes et leur correction et compare cette valeur aux [*Affectation : repères définis par l'organisation*].

(4) L'organisation utilise des outils automatisés de gestion des rustines pour faciliter la correction des lacunes des [*Affectation : composantes de système définies par l'organisation*].

Références :

Aucune.

SI-3 PROTECTION CONTRE LE CODE MALVEILLANT

Contrôle :

(A) L'organisation utilise des mécanismes de protection contre le code malveillant aux points d'entrée et de sortie du système d'information et dans les postes de travail, les serveurs ou les dispositifs mobiles du réseau afin de détecter et d'éradiquer le code :

(a) Transmis par les pièces jointes de courrier électronique, les accès Web, les supports amovibles ou autres sources usuelles; ou

(b) Inoculé par l'exploitation des vulnérabilités du système d'information.

(B) L'organisation modifie les mécanismes de protection contre le code malveillant (incluant les définitions de signature) dès la diffusion des mises à jour, en conformité avec sa politique et ses procédures de gestion de l'information.

(C) L'organisation configure les mécanismes de protection contre le code malveillant de manière à :

(a) Effectuer des analyses périodiques du système d'information [*Affectation : fréquence définie par l'organisation*] et des balayages en temps réel des fichiers de sources externes lors de leur téléchargement, de leur ouverture ou de leur exécution, en conformité avec sa politique de sécurité; et

(b) [*Sélection (un ou plusieurs): bloque le code malveillant; met le code malveillant en quarantaine, envoie une alerte à l'administrateur; [Affectation : mesure définie par l'organisation action]*] lors de la détection de code malveillant.

(D) L'organisation traite les faux positifs résultant de la détection et de l'éradication de code malveillant et leurs répercussions potentielles sur la disponibilité du système d'information.

Conseils supplémentaires : Les points d'entrée et de sortie du système d'information incluent, par exemple, les pare-feu, serveurs de courrier électronique, serveurs Web, serveurs mandataires et serveurs d'accès à distance. Le code malveillant inclut, par exemple, les virus, les vers, les chevaux de Troie et les espiogiciels. Il peut également être codé en différents formats (UUENCODE, Unicode, etc.) ou contenu dans un fichier comprimé. Les supports amovibles incluent, par exemple, les clés USB, les disquettes ou les disques compacts. Il existe une variété de technologies et de méthodes pour limiter ou éliminer les effets des attaques de code malveillant. Une gestion omniprésente de la configuration et des contrôles stricts d'intégrité du logiciel peuvent prévenir efficacement l'exécution de codes non autorisés. En plus du logiciel commercial standard, le code malveillant peut également se retrouver dans le logiciel personnalisé. Il peut, par exemple, prendre la forme de bombes logiques, de portes dérobées et autres types de cyberattaque capables de mettre en péril les missions et les fonctions opérationnelles de l'organisation. Les mécanismes traditionnels de protection ne sont pas conçus pour détecter ce type de code. Dans ces situations, pour s'assurer que le logiciel n'exécute pas de fonctions autres que celles prévues, les organisations doivent plutôt compter sur d'autres mesures d'atténuation du risque (pratiques de codage sécurisées, processus d'approvisionnement fiables, contrôle et gestion de la configuration et pratiques de surveillance). Contrôles connexes : SA-4, SA-8, SA-12, SA-13, SI-4, SI-7.

Améliorations du contrôle :

(1) L'organisation centralise la gestion des mécanismes de protection contre le code malveillant.

(2) Le système met automatiquement à jour les mécanismes de protection contre le code malveillant (incluant les définitions de signature).

(3) Le système empêche les utilisateurs non privilégiés de contourner les mécanismes de protection contre le code malveillant.

(4) Le système met à jour les mécanismes de protection contre le code malveillant uniquement lorsqu'un utilisateur privilégié le demande.

(5) L'organisation ne permet pas aux utilisateurs d'insérer des supports amovibles dans le système.

(6) L'organisation teste les mécanismes de protection contre le code malveillant [*Affectation : fréquence définie par l'organisation*] en inoculant dans le système d'information un scénario de test bénin connu et non invasif pour ensuite vérifier qu'il y a effectivement, comme il se doit, détection du scénario et signalement des incidents qui lui sont associés.

Références :

Aucune.

SI-4 SURVEILLANCE DES SYSTÈMES D'INFORMATION

Contrôle :

(A) L'organisation surveille les événements liés au système d'information en conformité avec [*Affectation : objectifs de surveillance définis par l'organisation*] et détecte les attaques contre le système.

(B) L'organisation identifie les utilisations non autorisées du système d'information.

(C) L'organisation déploie dans le système d'information des dispositifs de surveillance à la fois (i) stratégiquement pour collecter l'information qu'elle juge essentielle et (ii) de manière aléatoire pour pister des types de transaction qui l'intéressent particulièrement.

(D) L'organisation relève le niveau des activités de surveillance du système d'information chaque fois qu'elle identifie un risque accru pour les activités et les biens de l'organisation, les individus, les autres organisations ou le Canada suite à la réception de renseignements, d'information concernant le respect des lois ou d'information en provenance d'autres sources crédibles.

(E) L'organisation obtient un avis juridique concernant les activités de surveillance du système d'information en conformité avec les lois du GC et les politiques, directives et normes du SCT.

Conseils supplémentaires : La surveillance du système d'information est à la fois externe et interne. La surveillance externe inclut l'observation des événements qui se produisent à la frontière du système (c.-à-d., défense du périmètre et protection des frontières). La surveillance interne inclut l'observation des événements qui se produisent à l'intérieur du système (p. ex., réseaux organisationnels internes et composantes de système). Cette capacité de surveillance est possible grâce à une variété d'outils et de techniques (systèmes de détection et de prévention des intrusions, logiciel de protection contre le code malveillant, logiciel de surveillance des dossiers de vérification, logiciel de surveillance des réseaux, etc.). Les dispositifs de surveillance sont insérés à des endroits stratégiques, par exemple, dans des emplacements particuliers du périmètre et près des batteries de serveurs qui hébergent des applications essentielles; les dispositifs sont normalement utilisés dans les interfaces gérées associées aux contrôles SC-7 et AC-17. La granularité de l'information collectée est déterminée par les objectifs de surveillance de l'organisation et la capacité du système de prendre en charge ces activités. Un exemple de type particulier de transaction que l'organisation est intéressée à surveiller est le trafic HTTP qui contourne les mandataires HTTP organisationnels alors que ces dispositifs doivent être utilisés. Contrôles connexes : AC-4, AC-8, AC-17, AU-2, AU-6, SI-3, SI-7.

Améliorations du contrôle :

(1) L'organisation utilise des protocoles communs pour interconnecter et configurer les outils individuels de détection en un mécanisme de détection d'intrusion systémique unique.

(2) L'organisation utilise des outils automatisés pour effectuer une analyse des événements en temps quasi réel.

(3) L'organisation utilise des outils automatisés pour intégrer les outils de détection d'intrusion aux mécanismes de contrôle d'accès et de flux pour contrer rapidement les attaques; les mécanismes peuvent alors être reconfigurés de manière à permettre l'isolation et l'élimination des attaques.

(4) Le système surveille les communications entrantes et sortantes pour détecter toute activité ou condition inhabituelles ou non autorisées.

Conseils supplémentaires d'amélioration : Les activités ou conditions inhabituelles ou non autorisées incluent, par exemple, le trafic interne qui indique la présence de code malveillant dans le système ou sa propagation dans les composantes, l'exportation non autorisée d'information et l'envoi d'un signal vers un système externe. Les preuves de l'existence de code malveillant permettent de découvrir que des systèmes ou leurs composantes sont potentiellement compromis.

(5) Le système produit des alertes en temps quasi réel lorsqu'il relève les indications de compromission réelle ou potentielle suivantes : [*Affectation : liste des indicateurs de compromission définie par l'organisation*].

Conseils supplémentaires d'amélioration : Les alertes peuvent provenir, selon la liste des indicateurs définie par l'organisation, d'une variété de sources, par exemple, de dossiers de vérification ou de données produites par les mécanismes de protection contre le code malveillant, de mécanismes de détection ou de prévention des intrusions ou de dispositifs de protection des frontières tels les pare-feu, les passerelles et les routeurs.

(6) Le système empêche les utilisateurs non privilégiés de contourner les capacités de détection et de prévention des intrusions.

(7) Le système informe [*Affectation : liste définie par l'organisation des employés (identifiés par nom et (ou) rôle) chargés d'intervenir en cas d'incident*] des événements suspects et prend les [*Affectation : liste définie par l'organisation des mesures les moins nuisibles d'interruption des événements suspects*].

Conseils supplémentaires d'amélioration : Les mesures les moins nuisibles peuvent inclure l'envoi d'une demande d'intervention du personnel.

(8) L'organisation protège l'information obtenue des outils de surveillance des intrusions contre tout accès non autorisé et toute modification et suppression.

(9) L'organisation teste et (ou) vérifie la capacité des outils de surveillance des intrusions [*Affectation : période définie par l'organisation*].

Conseils supplémentaires d'amélioration : La fréquence des tests et (ou) des vérifications est liée au type et à la méthode de déploiement des outils de surveillance des intrusions.

(10) L'organisation prend les mesures nécessaires pour rendre le trafic chiffré visible aux outils de surveillance du système d'information.

Conseils supplémentaires d'amélioration : L'amélioration reconnaît le besoin d'équilibrer le trafic de chiffrement par rapport au besoin de surveiller le contenu du trafic. Certaines organisations jugent essentiel d'assurer la confidentialité du trafic et d'autres, qu'il est plus important de protéger la mission.

(11) L'organisation analyse le trafic des communications sortantes à la frontière externe du système (c.-à-d., à son périmètre) et, le cas échéant, à certains de ses points intérieurs (p. ex., sous-réseaux, sous-systèmes) pour découvrir des anomalies.

Conseils supplémentaires d'amélioration : Les anomalies du système d'information incluent, par exemple, les transferts de fichiers volumineux, les connexions persistantes de longues durée, les protocoles et ports inhabituels utilisés et les tentatives de communications avec des adresses externes malveillantes suspectes.

(12) L'organisation utilise des mécanismes automatisés pour alerter le personnel de sécurité des répercussions potentielles des activités inhabituelles ou inappropriées suivantes : [*Affectation : liste définie par l'organisation des activités inhabituelles ou inappropriées qui déclenchent des alertes*].

(13) L'organisation :

(a) Analyse le trafic des communications et (ou) la tendance des événements du système d'information;

(b) Développe des profils des modèles de trafic et (ou) des événements; et

(c) Utilise les profils pour calibrer les dispositifs de surveillance afin de réduire le nombre de faux positifs à [*Affectation : mesure des faux positifs définie par l'organisation*] et le nombre de faux négatifs à [*Affectation : mesure des faux négatifs définie par l'organisation*].

(14) L'organisation utilise un système de détection d'intrusions sans fil pour identifier les dispositifs sans fil indésirables et détecter les tentatives d'attaque et les compromissions et (ou) brèches potentielles du système.

(15) L'organisation utilise un système de détection d'intrusions pour surveiller le trafic de communications sans fil lors de son passage dans le circuit des réseaux.

(16) L'organisation met en corrélation l'information obtenue des outils de surveillance utilisés dans l'ensemble du système pour développer une sensibilisation à la situation organisationnelle du système.

(17) L'organisation met en corrélation les résultats des activités de surveillance physique et logicielle et de la chaîne d'approvisionnement pour développer une sensibilisation intégrée à la situation du système.

Conseils supplémentaires d'amélioration : Une sensibilisation intégrée à la situation améliore la capacité de l'organisation de détecter plus rapidement les attaques sophistiquées et d'enquêter sur les méthodes et techniques utilisées.

Références :

Aucune.

SI-5 DIRECTIVES, ALERTES ET AVIS DE SÉCURITÉ

Contrôle :

(A) L'organisation reçoit régulièrement d'organisations externes désignées des alertes, avis et directives concernant le système d'information.

(B) L'organisation produit les alertes, avis et directives de sécurité internes qu'elle juge nécessaires.

(C) L'organisation diffuse des alertes, avis et directives de sécurité à [*Affectation : liste des employés (par nom et (ou) rôle) définie par l'organisation*].

(D) L'organisation applique des directives de sécurité à des intervalles prédéterminés ou informe les organisations émettrices du niveau de non-conformité.

Conseils supplémentaires : Le respect des directives de sécurité est essentiel compte tenu de la nature critique de plusieurs d'entre elles et des effets potentiels immédiats, sur les activités et les biens de l'organisation, les individus, les autres organisations et le Canada, du non-respect de leur calendrier de mise en œuvre.

Améliorations du contrôle :

(1) L'organisation utilise des mécanismes automatisés pour diffuser, au besoin, de l'information sur les alertes et les avis de sécurité à l'ensemble de l'organisation.

Références :

Aucune.

SI-6 VÉRIFICATION DE LA FONCTIONNALITÉ DE SÉCURITÉ

Contrôle :

(A) Le système d'information vérifie le bon fonctionnement des fonctions de sécurité [*Sélection (un ou plusieurs): [Affectation : états transitionnels du système définis par l'organisation]; à la demande d'un utilisateur qui possède les privilèges appropriés; périodiquement tous les [Affectation : période définie par l'organisation*] et [*Sélection (un ou plusieurs): informe l'administrateur de système; arrête le système; redémarre le système; [Affectation : autre(s) mesure(s) définie(s) par l'organisation]*] lorsque des anomalies sont relevées.

Conseils supplémentaires : Le besoin de vérifier la fonctionnalité de sécurité s'applique à toutes les fonctions de sécurité. Dans le cas des fonctions qui ne peuvent effectuer automatiquement d'autotests, l'organisation soit met en œuvre des contrôles de sécurité compensatoires, soit accepte explicitement le risque associé à la non-exécution de la vérification. Les états transitionnels de système incluent, par exemple, le démarrage, le redémarrage, l'arrêt et l'interruption.

Améliorations du contrôle :

(1) Le système produit des avis de non réussite des tests de sécurité automatisés.

(2) Le système offre un soutien automatisé de la gestion des tests de sécurité distribués.

(3) L'organisation signale le résultat de la vérification des fonctions de sécurité à ses agents désignés responsables de la sécurité de l'information.

Conseils supplémentaires d'amélioration : Les agents de l'organisation responsables de la sécurité de l'information incluent, par exemple, les agents principaux de sécurité de l'information, les gestionnaires de la sécurité des systèmes d'information et les agents de la sécurité des systèmes d'information.

Références :

Aucune.

SI-7 INTÉGRITÉ DE L'INFORMATION ET DU LOGICIEL

Contrôle :

(A) Le système d'information détecte les modifications non autorisées du logiciel et de l'information.

Conseils supplémentaires : L'organisation utilise de saines pratiques de génie logiciel pour les mécanismes d'intégrité commerciaux standard (p. ex., vérifications de la parité, vérifications cycliques de la redondance, hachages cryptographiques) et des outils pour surveiller automatiquement l'intégrité du système d'information et des applications qu'il héberge.

Améliorations du contrôle :

(1) L'organisation réévalue l'intégrité du logiciel et de l'information en effectuant [*Affectation : fréquence définie par l'organisation*] des analyses d'intégrité du système.

(2) L'organisation utilise des outils automatisés qui produisent des avis aux employés désignés lors de la découverte d'écarts durant la vérification de l'intégrité.

(3) L'organisation utilise des outils de vérification de l'intégrité gérés centralement.

(4) L'organisation exige l'utilisation d'emballages inviolables pour les [*Affectation : composantes de système définies par l'organisation*] durant [*Sélection : transport du fournisseur au site opérationnel; durant l'exploitation; les deux*].

Références :

Aucune.

SI-8 PROTECTION ANTI-POURRIEL

Contrôle :

(A) L'organisation utilise des mécanismes de protection antipourriels aux points d'entrée et de sortie du système d'information et dans les postes de travail, les serveurs ou les dispositifs mobiles de réseau pour détecter (et intervenir, le cas échéant) les messages non sollicités transmis par les courriels et leurs pièces jointes, les accès Web ou autres sources usuelles.

(B) L'organisation met à jour les mécanismes de protection antipourriels (incluant les définitions de signature) dès la diffusion de nouvelles versions, en conformité avec sa politique et ses procédures de gestion de l'information.

Conseils supplémentaires : Les points d'entrée et de sortie du système d'information incluent, par exemple, les pare-feu, les serveurs de courrier électronique, les serveurs Web, les serveurs mandataires et les serveurs d'accès à distance. Contrôles connexes : SC-5, SI-3.

Améliorations du contrôle :

(1) L'organisation centralise la gestion des mécanismes de protection antipourriels.

(2) Le système met automatiquement à jour les mécanismes de protection antipourriels (incluant les définitions de signature).

Références :

Aucune.

SI-9 RESTRICTIONS RELATIVES À LA SAISIE D'INFORMATION

Contrôle :

(A) L'organisation limite au personnel autorisé la capacité d'entrer de l'information dans le système d'information.

Conseils supplémentaires : Les restrictions visant le personnel autorisé à entrer de l'information dans le système d'information peuvent aller au delà des seuls contrôles d'accès du système et incluent des restrictions basées sur des responsabilités de projet et (ou) opérationnelles particulières. Contrôles connexes : AC-5, AC-6.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SI-10 VALIDATION DE LA SAISIE D'INFORMATION

Contrôle :

(A) Le système d'information vérifie la validité des entrées d'information.

Conseils supplémentaires : On a mis en place des règles de vérification de la validité de la syntaxe et des valeurs sémantiques des entrées (p. ex., jeu de caractères, longueur, plage numérique, valeurs acceptables) afin de s'assurer qu'elles respectent des définitions spécifiques en matière de format et de contenu. Les entrées transmises aux interpréteurs sont filtrées au préalable pour empêcher que leur contenu soit interprété accidentellement comme des commandes.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SI-11 TRAITEMENT DES ERREURS

Contrôle :

(A) Le système d'information identifie les conditions d'erreur potentielles liées à la sécurité.

(B) Le système d'information produit des messages d'erreur qui incluent l'information nécessaire sur les mesures correctrices sans révéler [*Affectation : information sensible ou potentiellement préjudiciable définie par l'organisation*] contenue dans les journaux d'erreurs et les messages administratifs qui pourrait être exploitée par des adversaires.

(C) Le système d'information révèle les messages d'erreur seulement au personnel autorisé.

Conseils supplémentaires : L'organisation accorde une attention particulière à la structure et au contenu des messages d'erreur. La mesure dans laquelle le système d'information peut identifier et traiter les conditions d'erreur est dictée par la politique de l'organisation et les exigences opérationnelles. L'information sensible inclut, par exemple, les numéros de compte, les numéros d'assurance sociale et les numéros de carte de crédit.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SI-12 TRAITEMENT ET CONSERVATION DES SORTIES D'INFORMATION

Contrôle :

(A) L'organisation traite et conserve l'information interne et celle produite par le système d'information en conformité avec les lois du GC, les politiques, directives et normes concernées du SCT et les exigences opérationnelles.

Conseils supplémentaires : Les exigences de traitement et de conservation des sorties s'appliquent à l'ensemble du cycle de vie de l'information et, dans certains cas, vont au delà de l'élimination du système d'information lui-même. Bibliothèque et Archives Canada donne des conseils sur la conservation des dossiers. Contrôles connexes : MP-2, MP-4.

Améliorations du contrôle :

Aucune.

Références :

Aucune.

SI-13 PRÉVENTION DES PANNES PRÉVISIBLES

Contrôle :

(A) L'organisation protège le système d'information contre tout préjudice en tenant compte de la durée moyenne de fonctionnement avant défaillance des [*Affectation : liste des composantes de système définie par l'organisation*] dans des environnements d'exploitation spécifiques.

(B) L'organisation fournit, au besoin, des composantes de remplacement et un mécanisme d'échange des rôles actifs et passifs des composantes.

Conseils supplémentaires : La durée moyenne de fonctionnement avant défaillance est avant tout un élément de fiabilité; ce contrôle met l'accent sur les défaillances potentielles de composantes particulières responsables des capacités de sécurité. Les taux de durée moyenne de fonctionnement avant défaillance sont justifiables et basés sur des considérations propres à l'installation et non sur des moyennes de l'industrie. Le transfert des responsabilités entre les composantes actives et passives ne compromet en rien la sûreté, l'état de préparation opérationnelle ni la sécurité (p. ex., les variables d'état sont préservées). La composante passive est accessible en permanence, sauf pendant une procédure de reprise après défaillance ou pour des motifs de maintenance. Contrôle connexe : CP-2.

Améliorations du contrôle :

(1) L'organisation met la composante hors service en transférant ses responsabilités à une composante de remplacement à l'intérieur de [*Affectation : fraction ou pourcentage définis par l'organisation*] de la durée moyenne de fonctionnement avant défaillance.

(2) L'organisation interdit l'exécution sans supervision d'un processus pendant plus de [*Affectation : durée définie par l'organisation*].

(3) L'organisation lance manuellement un transfert entre les composantes actives et passives au moins une fois par [*Affectation : fréquence définie par l'organisation*] si la durée moyenne de fonctionnement avant défaillance est supérieure à [*Affectation : durée définie par l'organisation*].

(4) L'organisation, lors de la détection d'une défaillance d'une composante de système d'information :

(a) S'assure que la composante passive remplit avec succès et de manière transparente son rôle pendant [*Affectation : durée définie par l'organisation*]; et

(b) [*Sélection (un ou plusieurs): active [Affectation : alarme définie par l'organisation]; arrête automatiquement le système*].

Conseils supplémentaires d'amélioration : Le transfert automatique ou manuel des rôles à une unité passive peut se produire dès la détection d'une défaillance de composante.

Références :

Aucune.

5. Références

Référence n°	Titre du document	Contrôles de sécurité concernés
[Référence 1]	Secrétariat du Conseil du Trésor du Canada, Politique sur la sécurité du gouvernement (PSG), 1 juillet 2009.	S. o.
[Référence 2]	National Institute of Standards and Technology (NIST), Special Publication 800-53, Revision 3 Final Recommended Security Controls for Federal Information Systems, août 2009, incluant les mises à jour du 05-01-2010.	S. o.
[Référence 3]	Travaux publics et Services gouvernementaux Canada, Manuel de la sécurité industrielle, juillet 2009.	PE-3, PS-3
[Référence 4]	Centre de la sécurité des télécommunications Canada et Gendarmerie royale du Canada, Méthodologie harmonisée d'évaluation des menaces et des risques (TRA-1), octobre 2007.	RA-3
[Référence 5]	National Institute of Standards and Technology (NIST), FIPS PUB 200, Minimum Security Control Requirements for Federal Information and Information Systems, version finale, 9 mars 2006.	S. o.
[Référence 6]	Secrétariat du Conseil du Trésor du Canada, Politique d'utilisation des réseaux électroniques, 12 février 1998.	AC-8
[Référence 7]	Secrétariat du Conseil du Trésor du Canada, Norme opérationnelle sur la sécurité matérielle, 1er décembre 2004.	AC-17, CP-9, MP-1, MP-5, PE-1, PE-2, PE-3, PE-17
[Référence 8]	Secrétariat du Conseil du Trésor du Canada, Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information, 31 mai 2004.	AC-1, AC-17, AC-19, AT-1, AT-2, AU-1, AU-6, CA-1, CA-2, CA-5, CA-6, CM-1, CP-1, CP-2, CP-9, CP-10, IA-1, IR-1, IR-5, MA-1, MP-1, PE-1, PL-1, PL-2, PM-1, PM-2, PS-1, RA-1, SA-1, SA-2, SA-3, SC-1, SC-9, SI-1
[Référence 9]	Centre de la sécurité des télécommunications Canada, Algorithmes cryptographiques approuvés par le CSTC pour la protection des renseignements désignés PROTÉGÉ et pour les applications d'authentification et d'autorisation électroniques au sein du gouvernement du Canada (ITSA-11D), juillet 2008.	IA-7, MP-5, SA-4, SC-9, SC-12, SC-13
[Référence 10]	Secrétariat du Conseil du Trésor du Canada, Norme sur la sécurité du personnel, 17 octobre 2002.	PS-2, PS-3, PS-4, PS-5, PS-7
[Référence 11]	Secrétariat du Conseil du Trésor du Canada, Directive sur la gestion de la sécurité ministérielle, 1er juillet 2009.	CA-1, CA-2, CA-6, CA-7, PM-2, PM-4, PM-5
[Référence 12]	Secrétariat du Conseil du Trésor du Canada, Norme opérationnelle de sécurité - Programme de planification de la continuité des activités (PCA), 23 mars 2004.	AU-6, CP-1, CP-2
[Référence 13]	Secrétariat du Conseil du Trésor du Canada, Norme opérationnelle de sécurité - Niveaux de préparation des installations du gouvernement fédéral , 1er novembre 2002.	CP-2, IR-1

Référence n°	**Titre du document**	**Contrôles de sécurité concernés**
[Référence 14]	Secrétariat du Conseil du Trésor du Canada, Norme Sécurité relative à l'organisation et l'administration, 1er juin 1995.	AC-21, IR-1, MP-3, RA-3
[Référence 15]	Centre de la sécurité des télécommunications Canada, Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada (ITSD-01), janvier 2005.	PE-19, SC-13
[Référence 16]	Gendarmerie royale du Canada, Guide d'équipement de sécurité (G1-001). (*Diffusion restreinte*)	MP-4, MP-6
[Référence 17]	Centre de la sécurité des télécommunications Canada, Effacement et déclassification des supports d'information électroniques (ITSG-06), juillet 2006.	MP-4, MP-6
[Référence 18]	Gendarmerie royale du Canada, Norme pour le transport ou la transmission de renseignements et de biens de nature délicate (G1-009), décembre 2006. (*Diffusion restreinte*)	MP-5
[Référence 19]	Centre de la sécurité des télécommunications Canada, ITSG-31 User Authentification Guidance for IT Systèmes, mars 2009.	AU-10, IA-2, IA-5, IA-7, IA-8, MA-4
[Référence 20]	Conseil national de recherches du Canada, Code national du bâtiment (CNB) 2005.	PE-3
[Référence 21]	Conseil national de recherches du Canada, Code national de prévention des incendies (CNPI) 2005.	PE-3
[Référence 22]	Gendarmerie royale du Canada, Éléments du Code national du bâtiment 1995 touchant la sécurité (G1-007), avril 1998.	PE-3
[Référence 23]	Centre de la sécurité des télécommunications Canada, Guide to Interconnecting Security Domains (ITSG-32), 2010.	AC-17, SA-4, SC-13
[Référence 24]	Gendarmerie royale du Canada, Pièces sécuritaires (G1-029), avril 2006. (*Diffusion restreinte*)	MP-4, PE-3
[Référence 25]	Secrétariat du Conseil du Trésor du Canada, Politique d'évaluation des facteurs relatifs à la vie privée, 2 mai 2002.	PL-5
[Référence 26]	Secrétariat du Conseil du Trésor du Canada, Norme de sécurité et de gestion des marchés, 09 juin 1996.	PS-7, SA-4, SA-9
[Référence 27]	Centre de la sécurité des télécommunications Canada, Évaluation des vulnérabilités des assistants numériques personnels (PDA) (ITSPSR-18), octobre 2002.	AC-18, AC-19
[Référence 28]	Centre de la sécurité des télécommunications Canada, Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21), mai 2009.	AC-18, AC-19
[Référence 29]	Centre de la sécurité des télécommunications Canada, Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B (ITSB-40).	IA-7, MP-5, SA-4, SC-9, SC-12, SC-13, SC-28
[Référence 30]	Secrétariat du Conseil du Trésor du Canada, Guide de vérification – Sécurité des technologies de l'information, septembre 1995.	PL-2
[Référence 31]	Centre de la sécurité des télécommunications Canada, ITSA-23 Vendor Support for Security Products, janvier 2002.	MA-5

Référence n°	**Titre du document**	**Contrôles de sécurité concernés**
[Référence 32]	Centre de la sécurité des télécommunications Canada, Vulnérabilité sur le plan de la sécurité – Ordinateurs portatifs équipés de la technologie WLAN (ITSB-15), février 2004.	AC-18, AC-19
[Référence 33]	Centre de la sécurité des télécommunications Canada, Mesures de sécurité – Appareils électroniques sans fil (ITSB-19), mai 2004.	AC-18, AC-19
[Référence 34]	Centre de la sécurité des télécommunications Canada, Sécurité de la messagerie BlackBerry NIP à NIP (ITSB-57), octobre 2008.	AC-18, AC-19
[Référence 35]	Centre de la sécurité des télécommunications Canada, Conseils sur l'utilisation du protocole TLS (Transport Layer Security) au sein du gouvernement du Canada (ITSB-60), novembre 2008.	AC-18, IA-2
[Référence 36]	Centre de la sécurité des télécommunications Canada, Critères pour la conception, la fabrication, l'approvisionnement, l'installation et les essais de réception des enceintes blindées contre les radiofréquences (ITSG-02), août 1999.	AC-18, PE-18
[Référence 37]	Centre de la sécurité des télécommunications Canada, Manuel de contrôle du matériel COMSEC (ITSG-10), juillet 2006.	AU-1, AU-2, AU-3, AU-6, AU-9, CP-1, CP-2, IR-1, IR-4, IR-6, MP-1, MP-5, MP-6, PE-2, PE-3, SC-12
[Référence 38]	Centre de la sécurité des télécommunications Canada, Planification des installations COMSEC – Conseils et critères (ITSG-11), septembre 2002.	PE-19
[Référence 39]	Centre de la sécurité des télécommunications Canada, Procédures d'évaluation des installations du gouvernement du Canada (ITSG-12), septembre 2005.	PE-19
[Référence 40]	Centre de la sécurité des télécommunications Canada, Manuel sur la commande de clés cryptographiques (ITSG-13), mai 2006.	SC-12
[Référence 41]	Centre de la sécurité des télécommunications Canada, Sécurité de base recommandée pour Windows Serveur 2003 (ITSG-20), mars 2004.	CM-6
[Référence 42]	Centre de la sécurité des télécommunications Canada, Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22), juin 2007.	AC-4, CA-3, SC-3, SC-5, SC-7, SC-14
[Référence 43]	Centre de la sécurité des télécommunications Canada, Isolation d'un serveur d'entreprise Blackberry dans un environnement Microsoft Exchange (ITSG-23), mars 2007.	CM-6, SC-3, SC-7
[Référence 44]	Centre de la sécurité des télécommunications Canada, Établissement des zones de sécurité dans un réseau – Considérations en matière de positionnement des services au sein de zones spécifiques (ITSG-38), mai 2009.	CA-3, SC-3, SC-7, SC-14
[Référence 45]	Gendarmerie royale du Canada, Produits de réécriture des supports de TI et d'effacement sécurisé (B2-002), mai 2009.	MP-6
[Référence 46]	Gendarmerie royale du Canada, Guide pour la préparation d'un énoncé de sécurité matérielle (G1-005), janvier 2000.	PE-2, PE-3, PE-4
[Référence 47]	Gendarmerie royale du Canada, Cartes d'identité / Insignes d'accès (G1-006), juillet 2006.	PE-2
[Référence 48]	Gendarmerie royale du Canada, Scellage de protection des clés d'urgence	PE-3

Référence n°	**Titre du document**	**Contrôles de sécurité concernés**
	et passe-partout ou des serrures à code d'immeubles (G1-007).	
[Référence 49]	Gendarmerie royale du Canada, Lignes directrices visant les services de gardiens (G1-008), avril 2001	PE-3
[Référence 50]	Gendarmerie royale du Canada, Les systèmes de clés maitresses (G1-016), décembre 1981.	PE-3
[Référence 51]	Gendarmerie royale du Canada, Contrôle de l'accès (G1-024), août 2004.	PE-2, PE-3, PE-16
[Référence 52]	Gendarmerie royale du Canada, Protection, détection et intervention (G1-025), décembre 2004. (*Diffusion restreinte*)	PE-1, PE-2, PE-3, PE-6
[Référence 53]	Gendarmerie royale du Canada, Établissement des zones de sécurité matérielle (G1-026), septembre 2005.	PE-3, PE-4, PE-5
[Référence 54]	Gendarmerie royale du Canada, Protection matérielle des serveurs informatiques (G1-031), mars 2008.	PE-3
[Référence 55]	Gendarmerie royale du Canada, Lignes directrices sur l'élimination et la destruction des renseignements protégés sur disques durs (G2-003), octobre 2003.	MP-6
[Référence 56]	Director of Central Intelligence, Directive 6/9 Physical Security Standards for Sensitive Compartmented Information Facilities, novembre 2002.	SC-101
[Référence 57]	National Telecommunications Security Working Group, TSG Standard 2 Guidelines for Computerized Telephone Systems, mars 1990.	SC-101
[Référence 58]	National Telecommunications Security Working Group, TSG Standard 6 TSG-Approved Equipment, juin 2006.	SC-101
[Référence 59]	Centre de la sécurité des télécommunications Canada, Guide de gestion des risques de sécurité des systèmes d'information (ITSG-33), ÉBAUCHE.	PM-4, PM-9, PM-10
[Référence 60]	Centre de la sécurité des télécommunications Canada, Annexe 2 du Guide de gestion des risques de sécurité des systèmes d'information – Processus de mise en œuvre de la sécurité de l'information (ITSG-33), ÉBAUCHE.	CA-5, RA-2, RA-3, SA-13

5.1 Références supplémentaires

Cette section établit une correspondance entre les publications de tiers (non gouvernementales) et les publications sur la sécurité de l'information et les contrôles de sécurité mentionnées dans ce document. Les praticiens de la sécurité, lorsqu'il n'existe aucune publication équivalente du GC, peuvent consulter ces publications pour la conception, la mise en œuvre et la sélection de solutions de sécurité. Au fur et à mesure que des documents équivalents du GC deviendront disponibles, la section des références sera mise à jour.

Titre du document	**Contrôles de sécurité concernés**
NIST Special Publication 800-16 Revision 1 (ébauche) Information Security Training Requirements: A Role- and Performance-Based Model, mars 2009.	AT-1, AT-2, AT-3
NIST Special Publication 800-34 Rev.1 (ébauche) Contingency Planning Guide for Federal Information Systems, octobre 2009.	CP-1, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, IR-1, IR-2, IR-3, IR-8, RA-3, PL-6
NIST Special Publication 800-57 (ébauche) Recommendation for Key Management Part 3: Application-Specific Key Management Guidance, août 2008.	AC-3, IA-2, IA-5, IA-6, IA-8, MP-2, MP-4, MP-5, SC-8, SC-9, SC-12, SC-13, SC-17, SC-20, SC-21, NC-1
NIST Special Publication 800-61r1 Computer Security Incident Handling Guide, mars 2008.	Tous les contrôles des familles AU et IR.
NIST Special Publication 800-81r1 (ébauche) Secure Domaine Name System Deployment Guide, février 2009.	SC-20, SC-21, SC-22
NIST Special Publication 800-118 (ébauche) Guide to Entreprise Password Management, avril 2009.	AC-3, AC-7, IA-5, IA-6

Appendice A – Relation entre les contrôles et les objectifs de sécurité

Le Tableau 3 indique la relation entre les contrôles et les objectifs de sécurité (confidentialité, intégrité et disponibilité).

Tableau 3 – Relation entre les contrôles et les objectifs de sécurité

Id.	Amélioration	Nom	C	I	D
AC-1		Politique et procédures de contrôle d'accès	X	X	X
AC-2		Gestion des comptes	X	X	
AC-2	1	Gestion des comptes	X	X	
AC-2	2	Gestion des comptes	X	X	
AC-2	3	Gestion des comptes	X	X	
AC-2	4	Gestion des comptes	X	X	
AC-2	5	Gestion des comptes	X	X	
AC-2	6	Gestion des comptes	X	X	
AC-2	7	Gestion des comptes	X	X	
AC-3		Application des droits d'accès	X	X	
AC-3	1	[ANNULÉ]	-	-	-
AC-3	2	Application des droits d'accès	X	X	
AC-3	3	Application des droits d'accès	X	X	
AC-3	4	Application des droits d'accès	X	X	
AC-3	5	Application des droits d'accès	X	X	
AC-3	6	Application des droits d'accès	X	X	
AC-4		Application des contrôles des flux d'information	X	X	
AC-4	1	Application des contrôles des flux d'information	X	X	
AC-4	2	Application des contrôles des flux d'information	X	X	
AC-4	3	Application des contrôles des flux d'information	X	X	
AC-4	4	Application des contrôles des flux d'information	X	X	
AC-4	5	Application des contrôles des flux d'information	X	X	
AC-4	6	Application des contrôles des flux d'information	X	X	
AC-4	7	Application des contrôles des flux d'information	X	X	
AC-4	8	Application des contrôles des flux d'information	X	X	
AC-4	9	Application des contrôles des flux d'information	X	X	
AC-4	10	Application des contrôles des flux d'information	X	X	
AC-4	11	Application des contrôles des flux d'information	X	X	

Id.	Amélioration	Nom	C	I	D
AC-4	12	Application des contrôles des flux d'information	X	X	
AC-4	13	Application des contrôles des flux d'information	X	X	
AC-4	14	Application des contrôles des flux d'information	X	X	
AC-4	15	Application des contrôles des flux d'information	X	X	
AC-4	16	Application des contrôles des flux d'information	X	X	
AC-4	17	Application des contrôles des flux d'information	X	X	
AC-5		Séparation des tâches	X	X	
AC-6		Privilège minimum	X	X	
AC-6	1	Privilège minimum	X	X	
AC-6	2	Privilège minimum	X	X	
AC-6	3	Privilège minimum	X	X	
AC-6	4	Privilège minimum	X	X	
AC-6	5	Privilège minimum	X	X	
AC-6	6	Privilège minimum	X	X	
AC-7		Tentatives de connexion non réussies	X	X	X
AC-7	1	Tentatives de connexion non réussies	X	X	
AC-7	2	Tentatives de connexion non réussies	X		
AC-8		Avis concernant l'utilisation du système	X	X	
AC-9		Avis concernant les connexions antérieures (accès)		X	
AC-9	1	Avis concernant les connexions antérieures (accès)		X	
AC-9	2	Avis concernant les connexions antérieures (accès)		X	
AC-9	3	Avis concernant les connexions antérieures (accès)		X	
AC-10		Contrôle des sessions simultanées		X	
AC-11		Verrouillage de session	X	X	
AC-11	1	Verrouillage de session	X		
AC-12		[ANNULÉ]	-	-	-
AC-13		[ANNULÉ]	-	-	-
AC-14		Opérations permises sans identification ni authentification	X	X	
AC-14	1	Opérations permises sans identification ni authentification	X	X	
AC-15		[ANNULÉ]	-	-	-
AC-16		Attributs de sécurité	X	X	
AC-16	1	Attributs de sécurité	X	X	
AC-16	2	Attributs de sécurité		X	
AC-16	3	Attributs de sécurité		X	
AC-16	4	Attributs de sécurité	X	X	
AC-16	5	Attributs de sécurité	X		

Id.	Amélioration	Nom	C	I	D
AC-17		Accès à distance	X	X	
AC-17	1	Accès à distance	X	X	
AC-17	2	Accès à distance	X	X	
AC-17	3	Accès à distance	X	X	
AC-17	4	Accès à distance	X	X	
AC-17	5	Accès à distance	X	X	
AC-17	6	Accès à distance	X		
AC-17	7	Accès à distance	X	X	
AC-17	8	Accès à distance	X	X	
AC-18		Accès sans fil	X	X	
AC-18	1	Accès sans fil	X	X	
AC-18	2	Accès sans fil	X	X	
AC-18	3	Accès sans fil	X	X	
AC-18	4	Accès sans fil	X	X	
AC-18	5	Accès sans fil	X	X	
AC-18	100	Accès sans fil	X	X	
AC-19		Contrôle d'accès aux dispositifs mobiles	X	X	
AC-19	1	Contrôle d'accès aux dispositifs mobiles	X		
AC-19	2	Contrôle d'accès aux dispositifs mobiles	X	X	
AC-19	3	Contrôle d'accès aux dispositifs mobiles	X	X	
AC-19	4	Contrôle d'accès aux dispositifs mobiles	X		
AC-20		Utilisation des systèmes d'information externes	X	X	
AC-20	1	Utilisation des systèmes d'information externes	X	X	
AC-20	2	Utilisation des systèmes d'information externes	X		
AC-21		Collaboration et partage d'information entre utilisateurs	X		
AC-21	1	Collaboration et partage d'information entre utilisateurs	X		
AC-21	100	Collaboration et partage d'information entre utilisateurs	X	X	
AC-22		Contenu accessible au public	X		
AT-1		Politique et procédures de formation et de sensibilisation à la sécurité	X	X	X
AT-2		Sensibilisation à la sécurité	X	X	X
AT-2	1	Sensibilisation à la sécurité	X	X	X
AT-3		Formation à la sécurité	X	X	X
AT-3	1	Formation à la sécurité			X
AT-3	2	Formation à la sécurité	X	X	X
AT-4		Dossiers de formation à la sécurité	X	X	X
AT-5		Contacts avec les groupes et associations de sécurité	X	X	X

Id.	Amélioration	Nom	C	I	D
AU-1		Politique et procédures de vérification et de responsabilisation	X	X	X
AU-2		Événements vérifiables	X	X	
AU-2	1	[ANNULÉ]	-	-	
AU-2	2	[ANNULÉ]	-	-	
AU-2	3	Événements vérifiables	X	X	
AU-2	4	Événements vérifiables	X	X	
AU-3		Contenu des dossiers de vérification	X	X	
AU-3	1	Contenu des dossiers de vérification	X	X	
AU-3	2	Contenu des dossiers de vérification	X	X	
AU-4		Capacité de stockage des vérifications			X
AU-5		Intervention en cas de problèmes de traitement			X
AU-5	1	Intervention en cas de problèmes de traitement			X
AU-5	2	Intervention en cas de problèmes de traitement			X
AU-5	3	Intervention en cas de problèmes de traitement			X
AU-5	4	Intervention en cas de problèmes de traitement	X	X	
AU-6		Examen, analyse et rapports de vérification	X	X	
AU-6	1	Examen, analyse et rapports de vérification	X	X	
AU-6	2	[ANNULÉ]	-	-	-
AU-6	3	Examen, analyse et rapports de vérification	X	X	
AU-6	4	Examen, analyse et rapports de vérification	X	X	
AU-6	5	Examen, analyse et rapports de vérification	X	X	
AU-6	6	Examen, analyse et rapports de vérification	X	X	
AU-6	7	Examen, analyse et rapports de vérification	X	X	
AU-6	8	[ANNULÉ]	-	-	-
AU-6	9	Examen, analyse et rapports de vérification	X	X	
AU-7		Réduction des vérifications et production des rapports	X	X	
AU-7	1	Réduction des vérifications et production des rapports	X	X	
AU-8		Timbres horodateurs		X	
AU-8	1	Timbres horodateurs		X	
AU-9		Protection de l'information de vérification	X	X	
AU-9	1	Protection de l'information de vérification		X	
AU-9	2	Protection de l'information de vérification			X
AU-9	3	Protection de l'information de vérification		X	
AU-9	4	Protection de l'information de vérification		X	
AU-10		Non-répudiation		X	
AU-10	1	Non-répudiation		X	

Id.	Amélioration	Nom	C	I	D
AU-10	2	Non-répudiation		X	
AU-10	3	Non-répudiation		X	
AU-10	4	Non-répudiation		X	
AU-10	5	Non-répudiation		X	
AU-11		Conservation des dossiers de vérification			X
AU-12		Production des dossiers de vérification	X	X	X
AU-12	1	Production des dossiers de vérification		X	
AU-12	2	Production des dossiers de vérification		X	
AU-13		Surveillance de la divulgation d'information	X		
AU-14		Vérification des sessions			X
AU-14	1	Vérification des sessions			X
CA-1		Politique et procédures d'évaluation et d'autorisation de la sécurité	X	X	X
CA-2		Évaluations de la sécurité	X	X	X
CA-2	1	Évaluations de la sécurité	X	X	X
CA-2	2	Évaluations de la sécurité	X	X	X
CA-3		Connexions des systèmes d'information	X	X	
CA-3	1	Connexions des systèmes d'information	X		
CA-3	2	Connexions des systèmes d'information	X		
CA-4		[ANNULÉ]	-	-	-
CA-5		Plan de mise en œuvre des mesures de protection (Plan d'action et jalons)	X	X	X
CA-5	1	Plan de mise en œuvre des mesures de protection (Plan d'action et jalons)	X	X	X
CA-6		Autorisation de sécurité	X	X	X
CA-7		Surveillance permanente	X	X	X
CA-7	1	Surveillance permanente	X	X	X
CA-7	2	Surveillance permanente	X	X	X
CM-1		Politique et procédures de gestion de la configuration	X	X	
CM-2		Configuration de base		X	
CM-2	1	Configuration de base		X	
CM-2	2	Configuration de base		X	
CM-2	3	Configuration de base		X	
CM-2	4	Configuration de base		X	
CM-2	5	Configuration de base		X	
CM-2	6	Configuration de base		X	
CM-3		Contrôle des modifications de la configuration		X	
CM-3	1	Contrôle des modifications de la configuration		X	

Id.	Amélioration	Nom	C	I	D
CM-3	2	Contrôle des modifications de la configuration		X	
CM-3	3	Contrôle des modifications de la configuration		X	
CM-3	4	Contrôle des modifications de la configuration		X	
CM-4		Analyse des répercussions sur la sécurité		X	
CM-4	1	Analyse des répercussions sur la sécurité		X	
CM-4	2	Analyse des répercussions sur la sécurité		X	
CM-5		Restrictions d'accès associées aux modifications		X	
CM-5	1	Restrictions d'accès associées aux modifications		X	
CM-5	2	Restrictions d'accès associées aux modifications		X	
CM-5	3	Restrictions d'accès associées aux modifications		X	
CM-5	4	Restrictions d'accès associées aux modifications		X	
CM-5	5	Restrictions d'accès associées aux modifications		X	
CM-5	6	Restrictions d'accès associées aux modifications		X	
CM-5	7	Restrictions d'accès associées aux modifications		X	
CM-6		Paramètres de configuration		X	
CM-6	1	Paramètres de configuration		X	
CM-6	2	Paramètres de configuration		X	
CM-6	3	Paramètres de configuration		X	
CM-6	4	Paramètres de configuration		X	
CM-7		Fonctionnalité minimale	X	X	
CM-7	1	Fonctionnalité minimale	X	X	
CM-7	2	Fonctionnalité minimale	X	X	
CM-7	3	Fonctionnalité minimale	X	X	
CM-8		Inventaire des composantes de système d'information		X	
CM-8	1	Inventaire des composantes de système d'information		X	
CM-8	2	Inventaire des composantes de système d'information		X	
CM-8	3	Inventaire des composantes de système d'information		X	
CM-8	4	Inventaire des composantes de système d'information		X	
CM-8	5	Inventaire des composantes de système d'information		X	
CM-8	6	Inventaire des composantes de système d'information		X	
CM-9		Plan de gestion de la configuration		X	
CM-9	1	Plan de gestion de la configuration		X	
CP-1		Politique et procédures de planification d'urgence	X	X	X
CP-2		Plan des mesures d'urgence			X
CP-2	1	Plan des mesures d'urgence			X
CP-2	2	Plan des mesures d'urgence			X

Id.	Amélioration	Nom	C	I	D
CP-2	3	Plan des mesures d'urgence			X
CP-2	4	Plan des mesures d'urgence			X
CP-2	5	Plan des mesures d'urgence			X
CP-2	6	Plan des mesures d'urgence			X
CP-3		Formation sur les situations d'urgence			X
CP-3	1	Formation sur les situations d'urgence			X
CP-3	2	Formation sur les situations d'urgence			X
CP-4		Tests et exercices relatifs au plan des mesures d'urgence			X
CP-4	1	Tests et exercices relatifs au plan des mesures d'urgence			X
CP-4	2	Tests et exercices relatifs au plan des mesures d'urgence			X
CP-4	3	Tests et exercices relatifs au plan des mesures d'urgence			X
CP-4	4	Tests et exercices relatifs au plan des mesures d'urgence			X
CP-5		[ANNULÉ]	-	-	-
CP-6		Autre sites de stockage			X
CP-6	1	Autre sites de stockage			X
CP-6	2	Autre sites de stockage			X
CP-6	3	Autre sites de stockage			X
CP-7		Site de traitement de secours			X
CP-7	1	Site de traitement de secours			X
CP-7	2	Site de traitement de secours			X
CP-7	3	Site de traitement de secours			X
CP-7	4	Site de traitement de secours			X
CP-7	5	Site de traitement de secours	X	X	X
CP-8		Services de télécommunications			X
CP-8	1	Services de télécommunications			X
CP-8	2	Services de télécommunications			X
CP-8	3	Services de télécommunications			X
CP-8	4	Services de télécommunications			X
CP-9		Sauvegarde des systèmes d'information	X	X	X
CP-9	1	Sauvegarde des systèmes d'information		X	X
CP-9	2	Sauvegarde des systèmes d'information		X	X
CP-9	3	Sauvegarde des systèmes d'information			X
CP-9	4	[ANNULÉ]	-	-	-
CP-9	5	Sauvegarde des systèmes d'information			X
CP-9	6	Sauvegarde des systèmes d'information			X
CP-10		Récupération et reconstitution des systèmes d'information			X

Id.	Amélioration	Nom	C	I	D
CP-10	1	[ANNULÉ]	-	-	-
CP-10	2	Récupération et reconstitution des systèmes d'information		X	X
CP-10	3	Récupération et reconstitution des systèmes d'information			X
CP-10	4	Récupération et reconstitution des systèmes d'information		X	X
CP-10	5	Récupération et reconstitution des systèmes d'information			X
CP-10	6	Récupération et reconstitution des systèmes d'information		X	X
IA-1		Politique et procédures d'identification et d'authentification	X	X	
IA-2		Identification et authentification (utilisateurs organisationnels)	X	X	
IA-2	1	Identification et authentification (utilisateurs organisationnels)	X	X	
IA-2	2	Identification et authentification (utilisateurs organisationnels)	X	X	
IA-2	3	Identification et authentification (utilisateurs organisationnels)	X	X	
IA-2	4	Identification et authentification (utilisateurs organisationnels)	X	X	
IA-2	5	Identification et authentification (utilisateurs organisationnels)	X	X	
IA-2	6	Identification et authentification (utilisateurs organisationnels)	X	X	
IA-2	7	Identification et authentification (utilisateurs organisationnels)	X	X	
IA-2	8	Identification et authentification (utilisateurs organisationnels)	X	X	
IA-2	9	Identification et authentification (utilisateurs organisationnels)	X	X	
IA-3		Identification et authentification des dispositifs	X	X	
IA-3	1	Identification et authentification des dispositifs	X	X	
IA-3	2	Identification et authentification des dispositifs	X	X	
IA-3	3	Identification et authentification des dispositifs	X	X	
IA-4		Gestion des identificateurs	X	X	
IA-4	1	Gestion des identificateurs	X	X	
IA-4	2	Gestion des identificateurs		X	
IA-4	3	Gestion des identificateurs		X	
IA-4	4	Gestion des identificateurs	X	X	
IA-4	5	Gestion des identificateurs	X	X	
IA-5		Gestion des authentifiants	X	X	
IA-5	1	Gestion des authentifiants	X	X	
IA-5	2	Gestion des authentifiants		X	
IA-5	3	Gestion des authentifiants		X	
IA-5	4	Gestion des authentifiants	X	X	
IA-5	5	Gestion des authentifiants	X	X	
IA-5	6	Gestion des authentifiants	X	X	
IA-5	7	Gestion des authentifiants	X		
IA-5	8	Gestion des authentifiants	X	X	

Id.	Amélioration	Nom	C	I	D
IA-6		Occultation des authentifiants	X		
IA-7		Authentification des modules cryptographiques	X	X	
IA-8		Identification et authentification (utilisateurs non organisationnels)	X	X	
IR-1		Politique et procédures d'intervention en cas d'incident	X	X	X
IR-2		Formation sur les interventions en cas d'incident	X	X	X
IR-2	1	Formation sur les interventions en cas d'incident	X	X	X
IR-2	2	Formation sur les interventions en cas d'incident	X	X	X
IR-3		Tests et exercices relatifs aux interventions en cas d'incident	X	X	X
IR-3	1	Tests et exercices relatifs aux interventions en cas d'incident	X	X	X
IR-4		Traitement des incidents	X	X	X
IR-4	1	Traitement des incidents	X	X	X
IR-4	2	Traitement des incidents	X	X	X
IR-4	3	Traitement des incidents	X	X	X
IR-4	4	Traitement des incidents	X	X	X
IR-4	5	Traitement des incidents	X	X	
IR-5		Surveillance des incidents	X	X	X
IR-5	1	Surveillance des incidents	X	X	X
IR-6		Signalement des incidents	X	X	X
IR-6	1	Signalement des incidents	X	X	X
IR-6	2	Signalement des incidents	X	X	X
IR-7		Assistance pour les interventions en cas d'incident	X	X	X
IR-7	1	Assistance pour les interventions en cas d'incident	X	X	X
IR-7	2	Assistance pour les interventions en cas d'incident	X	X	X
IR-8		Plan d'intervention en cas d'incident	X	X	X
MA-1		Politique et procédures de maintenance des systèmes	X	X	X
MA-2		Maintenance contrôlée	X	X	X
MA-2	1	Maintenance contrôlée	X	X	X
MA-2	2	Maintenance contrôlée	X	X	X
MA-3		Outils de maintenance		X	X
MA-3	1	Outils de maintenance		X	X
MA-3	2	Outils de maintenance		X	X
MA-3	3	Outils de maintenance	X		
MA-3	4	Outils de maintenance		X	
MA-4		Maintenance effectuée à distance		X	
MA-4	1	Maintenance effectuée à distance		X	
MA-4	2	Maintenance effectuée à distance		X	

Id.	Amélioration	Nom	C	I	D
MA-4	3	Maintenance effectuée à distance	X	X	X
MA-4	4	Maintenance effectuée à distance	X	X	
MA-4	5	Maintenance effectuée à distance		X	
MA-4	6	Maintenance effectuée à distance	X	X	
MA-4	7	Maintenance effectuée à distance		X	
MA-5		Personnel de maintenance	X	X	X
MA-5	1	Personnel de maintenance	X	X	X
MA-5	2	Personnel de maintenance	X	X	X
MA-5	3	Personnel de maintenance	X	X	X
MA-5	4	Personnel de maintenance	X	X	X
MA-6		Maintenance opportune			X
MP-1		Politique et procédures de protection des supports	X	X	X
MP-2		Accès aux supports	X		
MP-2	1	Accès aux supports	X	X	
MP-2	2	Accès aux supports	X	X	
MP-3		Marquage des supports	X		
MP-4		Entreposage des supports	X		
MP-4	1	Entreposage des supports	X		
MP-5		Transport des supports	X	X	
MP-5	1	[ANNULÉ]	-	-	-
MP-5	2	Transport des supports	X	X	
MP-5	3	Transport des supports	X	X	
MP-5	4	Transport des supports	X	X	
MP-6		Nettoyage des supports	X		
MP-6	1	Nettoyage des supports	X		
MP-6	2	Nettoyage des supports	X		
MP-6	3	Nettoyage des supports	X		
MP-6	4	Nettoyage des supports	X		
MP-6	5	Nettoyage des supports	X		
MP-6	6	Nettoyage des supports	X		
PE-1		Politique et procédures de protection physique et environnementale	X	X	X
PE-2		Autorisations d'accès physique	X	X	X
PE-2	1	Autorisations d'accès physique	X	X	X
PE-2	2	Autorisations d'accès physique	X	X	
PE-2	3	Autorisations d'accès physique	X		
PE-3		Contrôle d'accès physique	X	X	X

Id.	Amélioration	Nom	C	I	D
PE-3	1	Contrôle d'accès physique	X	X	
PE-3	2	Contrôle d'accès physique	X		
PE-3	3	Contrôle d'accès physique	X	X	
PE-3	4	Contrôle d'accès physique	X	X	
PE-3	5	Contrôle d'accès physique		X	
PE-3	6	Contrôle d'accès physique		X	
PE-4		Contrôle d'accès aux supports de transmission	X	X	
PE-5		Contrôle d'accès aux dispositifs de sortie	X		
PE-6		Surveillance de l'accès physique	X	X	X
PE-6	1	Surveillance de l'accès physique			X
PE-6	2	Surveillance de l'accès physique	X	X	X
PE-7		Contrôle des visiteurs	X	X	
PE-7	1	Contrôle des visiteurs	X	X	
PE-7	2	Contrôle des visiteurs	X	X	
PE-8		Dossiers d'accès	X	X	
PE-8	1	Dossiers d'accès			X
PE-8	2	Dossiers d'accès			X
PE-9		Équipement et câblage d'alimentation			X
PE-9	1	Équipement et câblage d'alimentation			X
PE-9	2	Équipement et câblage d'alimentation			X
PE-10		Arrêt d'urgence			X
PE-10	1	[ANNULÉ]	-	-	-
PE-11		Alimentation d'urgence			X
PE-11	1	Alimentation d'urgence			X
PE-11	2	Alimentation d'urgence			X
PE-12		Éclairage d'urgence			X
PE-12	1	Éclairage d'urgence			X
PE-13		Protection contre les incendies			X
PE-13	1	Protection contre les incendies			X
PE-13	2	Protection contre les incendies			X
PE-13	3	Protection contre les incendies			X
PE-13	4	Protection contre les incendies			X
PE-14		Contrôle de la température et de l'humidité			X
PE-14	1	Contrôle de la température et de l'humidité			X
PE-14	2	Contrôle de la température et de l'humidité			X
PE-15		Protection contre les dégâts d'eau			X

Id.	Amélioration	Nom	C	I	D
PE-15	1	Protection contre les dégâts d'eau			X
PE-16		Livraison et retrait	X		X
PE-17		Lieu de travail de secours	X	X	X
PE-18		Emplacement des composantes de système d'information			X
PE-18	1	Emplacement des composantes de système d'information			X
PE-19		Fuites d'information	X		
PE-19	1	Fuites d'information	X		
PL-1		Politique et procédures de planification de la sécurité	X	X	X
PL-2		Plan de sécurité des systèmes	X	X	X
PL-2	1	Plan de sécurité des systèmes	X	X	X
PL-2	2	Plan de sécurité des systèmes	X	X	X
PL-3		[ANNULÉ]	-	-	-
PL-4		Règles de conduite	X	X	X
PL-4	1	Règles de conduite	X		
PL-5		Évaluation des facteurs relatifs à la vie privée	X		
PL-6		Planification des activités relatives à la sécurité	X	X	X
PS-1		Politique et procédures de sécurité du personnel	X	X	X
PS-2		Catégorisation des postes	X	X	X
PS-3		Enquête de sécurité sur le personnel	X	X	
PS-3	1	Enquête de sécurité sur le personnel	X		
PS-3	2	Enquête de sécurité sur le personnel	X		
PS-4		Licenciement du personnel	X	X	X
PS-5		Transfert de personnel	X	X	X
PS-6		Ententes d'accès	X	X	
PS-6	1	Ententes d'accès	X	X	
PS-6	2	Ententes d'accès	X		
PS-7		Sécurité du personnel tiers	X	X	
PS-8		Sanctions imposées au personnel	X	X	X
RA-1		Politique et procédures d'évaluation des risques	X	X	X
RA-2		Catégories de sécurité	X	X	X
RA-3		Évaluation des risques	X	X	X
RA-4		[ANNULÉ]	-	-	-
RA-5		Analyse des vulnérabilités	X	X	X
RA-5	1	Analyse des vulnérabilités	X	X	X
RA-5	2	Analyse des vulnérabilités	X	X	X
RA-5	3	Analyse des vulnérabilités	X	X	X

Id.	Amélioration	Nom	C	I	D
RA-5	4	Analyse des vulnérabilités	X	X	X
RA-5	5	Analyse des vulnérabilités	X	X	X
RA-5	6	Analyse des vulnérabilités	X	X	X
RA-5	7	Analyse des vulnérabilités	X	X	X
RA-5	8	Analyse des vulnérabilités	X	X	X
RA-5	9	Analyse des vulnérabilités	X	X	X
SA-1		Politique et procédures d'acquisition des systèmes et des services	X	X	
SA-2		Affectation des ressources		X	
SA-3		Soutien du cycle de vie		X	
SA-4		Acquisitions		X	
SA-4	1	Acquisitions		X	
SA-4	2	Acquisitions		X	
SA-4	3	Acquisitions		X	
SA-4	4	Acquisitions		X	
SA-4	5	Acquisitions		X	
SA-4	6	Acquisitions		X	
SA-4	7	Acquisitions		X	
SA-5		Documentation des systèmes d'information		X	
SA-5	1	Documentation des systèmes d'information		X	
SA-5	2	Documentation des systèmes d'information		X	
SA-5	3	Documentation des systèmes d'information		X	
SA-5	4	Documentation des systèmes d'information		X	
SA-5	5	Documentation des systèmes d'information		X	
SA-6		Restrictions relatives à l'utilisation de logiciel	X	X	
SA-6	1	Restrictions relatives à l'utilisation de logiciel	X	X	
SA-7		Logiciel installé d'utilisateur		X	
SA-8		Principes d'ingénierie de la sécurité		X	
SA-9		Services de système d'information externes		X	
SA-9	1	Services de système d'information externes		X	
SA-10		Gestion de la configuration par les développeurs		X	
SA-10	1	Gestion de la configuration par les développeurs		X	
SA-10	2	Gestion de la configuration par les développeurs		X	
SA-11		Tests de sécurité effectués par les développeurs		X	
SA-11	1	Tests de sécurité effectués par les développeurs		X	
SA-11	2	Tests de sécurité effectués par les développeurs		X	
SA-11	3	Tests de sécurité effectués par les développeurs		X	

Id.	Amélioration	Nom	C	I	D
SA-12		Protection de la chaîne d'approvisionnement		X	
SA-12	1	Protection de la chaîne d'approvisionnement		X	
SA-12	2	Protection de la chaîne d'approvisionnement		X	
SA-12	3	Protection de la chaîne d'approvisionnement		X	
SA-12	4	Protection de la chaîne d'approvisionnement		X	
SA-12	5	Protection de la chaîne d'approvisionnement		X	
SA-12	6	Protection de la chaîne d'approvisionnement		X	
SA-12	7	Protection de la chaîne d'approvisionnement		X	
SA-13		Robustesse (fiabilité)		X	
SA-14		Composantes de système d'information essentielles		X	
SA-14	1	Composantes de système d'information essentielles		X	
SC-1		Politique et procédures de protection des systèmes et des communications	X	X	X
SC-2		Partitionnement des applications	X	X	
SC-2	1	Partitionnement des applications	X	X	
SC-3		Isolation des fonctions de sécurité	X	X	
SC-3	1	Isolation des fonctions de sécurité	X	X	
SC-3	2	Isolation des fonctions de sécurité	X	X	
SC-3	3	Isolation des fonctions de sécurité	X	X	
SC-3	4	Isolation des fonctions de sécurité	X	X	
SC-3	5	Isolation des fonctions de sécurité	X	X	
SC-4		Information contenue dans les ressources partagées	X		
SC-4	1	Information contenue dans les ressources partagées	X		
SC-5		Protection contre les dénis de service			X
SC-5	1	Protection contre les dénis de service			X
SC-5	2	Protection contre les dénis de service			X
SC-6		Priorité des ressources			X
SC-7		Protection des frontières	X	X	
SC-7	1	Protection des frontières	X	X	
SC-7	2	Protection des frontières	X	X	
SC-7	3	Protection des frontières	X	X	
SC-7	4	Protection des frontières	X	X	
SC-7	5	Protection des frontières	X	X	
SC-7	6	Protection des frontières	X		
SC-7	7	Protection des frontières	X	X	
SC-7	8	Protection des frontières	X	X	

Id.	Amélioration	Nom	C	I	D
SC-7	9	Protection des frontières	X	X	
SC-7	10	Protection des frontières	X		
SC-7	11	Protection des frontières		X	
SC-7	12	Protection des frontières	X	X	
SC-7	13	Protection des frontières	X	X	
SC-7	14	Protection des frontières	X	X	
SC-7	15	Protection des frontières	X	X	
SC-7	16	Protection des frontières	X		
SC-7	17	Protection des frontières		X	
SC-7	18	Protection des frontières	X	X	X
SC-7	100	Protection des frontières	X	X	X
SC-7	101	Protection des frontières	X	X	X
SC-8		Intégrité des transmissions		X	
SC-8	1	Intégrité des transmissions		X	
SC-8	2	Intégrité des transmissions		X	
SC-9		Confidentialité des transmissions	X		
SC-9	1	Confidentialité des transmissions	X		
SC-9	2	Confidentialité des transmissions	X		
SC-9	100	Confidentialité des transmissions			
SC-10		Déconnexion de réseau	X	X	
SC-11		Chemin de confiance		X	
SC-12		Établissement et gestion des clés de chiffrement	X	X	
SC-12	1	Établissement et gestion des clés de chiffrement			X
SC-12	2	Établissement et gestion des clés de chiffrement	X	X	
SC-12	3	Établissement et gestion des clés de chiffrement	X	X	
SC-12	4	Établissement et gestion des clés de chiffrement	X	X	
SC-12	5	Établissement et gestion des clés de chiffrement	X	X	
SC-13		Utilisation de la cryptographie	X	X	
SC-13	1	Utilisation de la cryptographie	X		
SC-13	2	Utilisation de la cryptographie	X		
SC-13	3	Utilisation de la cryptographie	X		
SC-13	4	Utilisation de la cryptographie		X	
SC-13	100	Utilisation de la cryptographie	X		
SC-13	101	Utilisation de la cryptographie	X		
SC-13	102	Utilisation de la cryptographie	X		
SC-13	103	Utilisation de la cryptographie	X		

Id.	Amélioration	Nom	C	I	D
SC-13	104	Utilisation de la cryptographie	X	X	X
SC-14		Protection de l'accès public		X	X
SC-15		Dispositifs d'informatique coopérative	X		
SC-15	1	Dispositifs d'informatique coopérative	X		
SC-15	2	Dispositifs d'informatique coopérative	X	X	
SC-15	3	Dispositifs d'informatique coopérative	X	X	
SC-16		Transmission des attributs de sécurité	X	X	
SC-16	1	Transmission des attributs de sécurité		X	
SC-17		Certificats d'infrastructure à clé publique	X	X	
SC-18		Code mobile		X	
SC-18	1	Code mobile		X	
SC-18	2	Code mobile		X	
SC-18	3	Code mobile		X	
SC-18	4	Code mobile		X	
SC-19		Voix sur IP	X	X	
SC-20		Service sécurisé de résolution de nom et (ou) d'adresse (source autorisée)		X	
SC-20	1	Service sécurisé de résolution de nom et (ou) d'adresse (source autorisée)		X	
SC-21		Service sécurisé de résolution de nom et (ou) d'adresse (résolveur récursif ou cache)		X	
SC-21	1	Service sécurisé de résolution de nom et (ou) d'adresse (résolveur récursif ou cache)		X	
SC-22		Architecture et fourniture de service de résolution de nom et (ou) d'adresse	X	X	X
SC-23		Authenticité des sessions		X	
SC-23	1	Authenticité des sessions		X	
SC-23	2	Authenticité des sessions		X	
SC-23	3	Authenticité des sessions		X	
SC-23	4	Authenticité des sessions		X	
SC-24		Défaillance dans un état connu	X	X	
SC-25		Nœuds légers		X	
SC-26		Pièges à pirates		X	
SC-26	1	Pièges à pirates		X	
SC-27		Applications indépendantes des systèmes d'exploitation		X	
SC-28		Protection de l'information inactive	X	X	
SC-28	1	Protection de l'information inactive	X	X	
SC-29		Hétérogénéité		X	

Id.	Amélioration	Nom	C	I	D
SC-30		Techniques de virtualisation		X	
SC-30	1	Techniques de virtualisation		X	
SC-30	2	Techniques de virtualisation		X	
SC-31		Analyse des voies clandestines	X		
SC-31	1	Analyse des voies clandestines	X		
SC-32		Partitionnement des systèmes d'information	X	X	
SC-33		Intégrité de la préparation des transmissions		X	
SC-34		Programmes exécutables non modifiables		X	
SC-34	1	Programmes exécutables non modifiables		X	
SC-34	2	Programmes exécutables non modifiables		X	
SC-100		Authentification des sources		X	
SC-100	1	Authentification des sources		X	
SC-100	2	Authentification des sources		X	
SC-100	3	Authentification des sources		X	
SC-101		Systèmes de télécommunications non classifiés dans les installations protégées	X		
SI-1		Politique et procédures d'intégrité de l'information et des systèmes	X	X	X
SI-2		Correction des lacunes		X	
SI-2	1	Correction des lacunes		X	
SI-2	2	Correction des lacunes		X	
SI-2	3	Correction des lacunes		X	
SI-2	4	Correction des lacunes		X	
SI-3		Protection contre le code malveillant		X	
SI-3	1	Protection contre le code malveillant		X	
SI-3	2	Protection contre le code malveillant		X	
SI-3	3	Protection contre le code malveillant		X	
SI-3	4	Protection contre le code malveillant		X	
SI-3	5	Protection contre le code malveillant		X	
SI-3	6	Protection contre le code malveillant		X	
SI-4		Surveillance des systèmes d'information		X	
SI-4	1	Surveillance des systèmes d'information		X	
SI-4	2	Surveillance des systèmes d'information		X	
SI-4	3	Surveillance des systèmes d'information		X	
SI-4	4	Surveillance des systèmes d'information	X	X	
SI-4	5	Surveillance des systèmes d'information		X	
SI-4	6	Surveillance des systèmes d'information		X	

Id.	Amélioration	Nom	C	I	D
SI-4	7	Surveillance des systèmes d'information		X	X
SI-4	8	Surveillance des systèmes d'information	X	X	X
SI-4	9	Surveillance des systèmes d'information		X	
SI-4	10	Surveillance des systèmes d'information	X	X	
SI-4	11	Surveillance des systèmes d'information	X		
SI-4	12	Surveillance des systèmes d'information	X	X	
SI-4	13	Surveillance des systèmes d'information	X	X	X
SI-4	14	Surveillance des systèmes d'information	X	X	
SI-4	15	Surveillance des systèmes d'information	X	X	
SI-4	16	Surveillance des systèmes d'information		X	
SI-4	17	Surveillance des systèmes d'information	X	X	
SI-5		Directives, alertes et avis de sécurité		X	
SI-5	1	Directives, alertes et avis de sécurité		X	
SI-6		Vérification de la fonctionnalité de sécurité		X	
SI-6	1	Vérification de la fonctionnalité de sécurité		X	
SI-6	2	Vérification de la fonctionnalité de sécurité		X	
SI-6	3	Vérification de la fonctionnalité de sécurité		X	
SI-7		Intégrité de l'information et du logiciel		X	
SI-7	1	Intégrité de l'information et du logiciel		X	
SI-7	2	Intégrité de l'information et du logiciel		X	
SI-7	3	Intégrité de l'information et du logiciel		X	
SI-7	4	Intégrité de l'information et du logiciel		X	
SI-8		Protection anti-pourriel		X	X
SI-8	1	Protection anti-pourriel		X	X
SI-8	2	Protection anti-pourriel		X	X
SI-9		Restrictions relatives à la saisie d'information		X	
SI-10		Validation de la saisie d'information		X	
SI-11		Traitement des erreurs		X	
SI-12		Traitement et conservation des sorties d'information	X	X	
SI-13		Prévention des pannes prévisibles			X
SI-13	1	Prévention des pannes prévisibles			X
SI-13	2	Prévention des pannes prévisibles			X
SI-13	3	Prévention des pannes prévisibles			X
SI-13	4	Prévention des pannes prévisibles			X